

EXHIBIT 1

REDACTED VERSION
OF EXHIBIT FILED
UNDER SEAL



Deposition of:

Oren Dor

January 13, 2021

In the Matter of:

Facebook v. BrandTotal

Veritext Legal Solutions

800-734-5292 | calendar-dmv@veritext.com |

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

FACEBOOK, INC., a Delaware)Case No.
corporation,)3:20-cv-07182-JCS
Plaintiff/Counterclaim Defendant)
vs.)
BRANDTOTAL LTD., an Israel)
corporation,)
and UNIMANIA, INC., a Delaware)
corporation)
Defendants/Counterclaim)
Plaintiffs)

- HIGHLY CONFIDENTIAL -

Remote Videotaped 30(b)(6) Deposition of
BrandTotal, Ltd. and Unimania, Inc.
through the testimony of Oren Dor
January 13, 2021
6:15 a.m.

Reported by: Bonnie L. Russo

<div>Page 50</div> <div>1</div> <div>[REDACTED]</div>	<div>[REDACTED]</div>
<div>[REDACTED]</div>	<div>[REDACTED]</div>

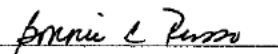
<p style="text-align: right;">Page 106</p> <p>1 [REDACTED]</p> <p>2 [REDACTED]</p> <p>3 [REDACTED]</p> <p>4 [REDACTED]</p> <p>5 [REDACTED]</p> <p>6 [REDACTED]</p> <p>7 [REDACTED]</p> <p>8 [REDACTED]</p> <p>9 [REDACTED]</p> <p>10 [REDACTED]</p> <p>11 [REDACTED]</p> <p>12 [REDACTED]</p> <p>13 [REDACTED]</p> <p>14 [REDACTED]</p> <p>15 [REDACTED]</p> <p>16 [REDACTED]</p> <p>17 [REDACTED]</p> <p>18 [REDACTED]</p> <p>19 [REDACTED]</p> <p>20 [REDACTED]</p> <p>21 [REDACTED]</p> <p>22 [REDACTED]</p>	<p style="text-align: right;">Page 108</p> <p>1 Can you explain to me how before it</p> <p>2 was suspended, UpVoice collected information</p> <p>3 from the Facebook site?</p> <p>4 A. Yes. So when a user is -- after</p> <p>5 installing UpVoice and accepting the terms of</p> <p>6 use and privacy policy and getting qualified,</p> <p>7 once he would visit Facebook.com, we would be</p> <p>8 collecting the different ad-related data that</p> <p>9 he sees on -- on his social feed.</p> <p>10 Q. So if the user navigates to the</p> <p>11 Facebook site, the UpVoice extension collects</p> <p>12 information that the user is viewing when they</p> <p>13 are on the Facebook site, correct?</p> <p>14 A. Yes.</p> <p>15 Q. And if the user is logged in using</p> <p>16 their user name and password so that they can</p> <p>17 access the Facebook site, then the UpVoice</p> <p>18 extension would collect the information that</p> <p>19 they are viewing at that time, correct?</p> <p>20 A. So with the user consent and after</p> <p>21 the user logs in, it would be collecting that</p> <p>22 user's data, yes.</p>
<p style="text-align: right;">Page 107</p> <p>1 A. Major publisher websites. We gave</p> <p>2 you the entire list.</p> <p>3 Q. Do you use these crawlers to collect</p> <p>4 information from the Facebook site?</p> <p>5 A. No.</p> <p>6 Q. Have you ever used these crawlers to</p> <p>7 collect information from the Facebook site?</p> <p>8 A. No.</p> <p>9 Q. Do you use these crawlers to collect</p> <p>10 information from the Instagram site?</p> <p>11 A. No.</p> <p>12 Q. On Page 2 of the -- of Exhibit 5,</p> <p>13 there are three methods identified: Consumer</p> <p>14 panel, public APIs, and avatars by segments,</p> <p>15 correct?</p> <p>16 A. Yes.</p> <p>17 Q. Are there any other methods used to</p> <p>18 collect information other than those three?</p> <p>19 A. No.</p> <p>20 Q. Can you explain to me how UpVoice</p> <p>21 collects data from -- sorry. Let me rephrase</p> <p>22 that.</p>	<p style="text-align: right;">Page 109</p> <p>1 Q. It would be collecting the data from</p> <p>2 the portion of the site they are viewing after</p> <p>3 having logged in?</p> <p>4 A. Yes.</p> <p>5 Q. Does the user need to log in to the</p> <p>6 Facebook site for the UpVoice extension to</p> <p>7 collect that information?</p> <p>8 A. Yes.</p> <p>9 Q. The UpVoice extension will collect</p> <p>10 information from the Facebook site regardless</p> <p>11 of whether the person using the browser is the</p> <p>12 same person who downloaded the UpVoice</p> <p>13 extension, correct?</p> <p>14 A. Depends on the extension. This is</p> <p>15 something we fixed with the October -- the new</p> <p>16 October or November UpVoice extensions.</p> <p>17 Q. Prior to October 2020, if the</p> <p>18 UpVoice extension was installed on a Chrome</p> <p>19 browser, then the UpVoice extension would</p> <p>20 collect information regardless of who was using</p> <p>21 the browser, correct?</p> <p>22 A. Yes. It would be collecting nonPII</p>

<p style="text-align: right;">Page 110</p> <p>1 information from whomever visits Facebook.com.</p> <p>2 Q. All of the information that the</p> <p>3 UpVoice extension collects, the UpVoice</p> <p>4 extension would collect regardless of who is</p> <p>5 using the browser, correct?</p> <p>6 MR. HAUER: Object to form.</p> <p>7 THE WITNESS: So, yes, for -- for</p> <p>8 versions earlier than October 2020.</p> <p>9 BY MR. HOLTZBLATT:</p> <p>10 Q. And you said that you -- this is</p> <p>11 something you fixed in October 2020. What do</p> <p>12 you mean by that?</p> <p>13 A. We pull -- we added an additional</p> <p>14 opt-in window that whenever a user navigates to</p> <p>15 Facebook.com or any other social platform, he</p> <p>16 gets an additional opt-in message asking him</p> <p>17 permission to -- for UpVoice to be collecting</p> <p>18 ad-related data with that specific account.</p> <p>19 Q. So is that permission prompt -- is</p> <p>20 it -- is it -- is it fair to call that a</p> <p>21 permission prompt?</p> <p>22 A. Permission opt-in, yes.</p>	<p style="text-align: right;">Page 112</p> <p>1 Q. So 10 to 15 percent of your users</p> <p>2 when they -- still when they visit the Facebook</p> <p>3 site, the UpVoice extension will collect</p> <p>4 information regardless of who is using the</p> <p>5 browser?</p> <p>6 MR. HAUER: Object to form.</p> <p>7 Mischaracterizes prior testimony.</p> <p>8 THE WITNESS: Yes.</p> <p>9 MR. HOLTZBLATT: Ryan, the standing</p> <p>10 order directs that you may object to form and</p> <p>11 only object to form.</p> <p>12 BY MR. HOLTZBLATT:</p> <p>13 Q. Please answer the question, Mr. Dor.</p> <p>14 A. Would you mind repeating the</p> <p>15 question.</p> <p>16 Q. For 10 to 15 percent of your users</p> <p>17 who have not had the earlier version of the</p> <p>18 UpVoice extension uninstalled, when they visit</p> <p>19 the Facebook site as of today, the UpVoice</p> <p>20 extension will still collect all of the</p> <p>21 information regardless of who is using the</p> <p>22 browser?</p>
<p style="text-align: right;">Page 111</p> <p>1 Q. Permission opt-in.</p> <p>2 A. An additional permission opt-in,</p> <p>3 yes. Okay.</p> <p>4 Q. For users whose version of UpVoice</p> <p>5 has now been uninstalled from their browser in</p> <p>6 October of 2020; does that permission opt-in</p> <p>7 appear?</p> <p>8 A. Say again.</p> <p>9 Q. Ten to fifteen percent of -- of your</p> <p>10 users have not had their -- the version of</p> <p>11 UpVoice uninstalled from their Chrome browser,</p> <p>12 correct?</p> <p>13 A. Yes.</p> <p>14 Q. Has the -- is the version of the</p> <p>15 UpVoice extension that is installed on those 10</p> <p>16 to 15 percent of users in, say, November of</p> <p>17 2020 when they visit the Facebook site, do they</p> <p>18 see a permission opt-in?</p> <p>19 A. The answer is no because we -- once</p> <p>20 an extension is taken down from the Chrome</p> <p>21 store, we don't have the ability to update the</p> <p>22 version of it.</p>	<p style="text-align: right;">Page 113</p> <p>1 A. Yes.</p> <p>2 Q. And you are still collecting -- you</p> <p>3 are still storing that information?</p> <p>4 A. Yes.</p> <p>5 Q. And you are still aggregating that</p> <p>6 information and providing it to customers as of</p> <p>7 today?</p> <p>8 A. Yes.</p> <p>9 Q. Does UpVoice collect only</p> <p>10 information that is visible to the user in</p> <p>11 their browser window?</p> <p>12 A. No. It also makes some background</p> <p>13 calls.</p> <p>14 Q. What is a background call?</p> <p>15 A. A background call is a call for --</p> <p>16 after the -- after user consents and logs in,</p> <p>17 it's a call to data that he either owns or has</p> <p>18 access to, and we would be collecting data from</p> <p>19 there.</p> <p>20 Q. These are calls that are made by the</p> <p>21 UpVoice extension to the Facebook server,</p> <p>22 correct?</p>

<p style="text-align: right;">Page 154</p> <p>1 become aware of the AdGuard report?</p> <p>2 A. We -- we -- we got to know the</p> <p>3 report a couple of days after it was published</p> <p>4 probably, let's say, five -- five days after it</p> <p>5 was published.</p> <p>6 Q. And how did you become aware of the</p> <p>7 AdGuard report?</p> <p>8 A. My CTO sent -- sent it to me.</p> <p>9 Q. On -- if you could scroll back to</p> <p>10 the top of the AdGuard -- of Exhibit 9 and go</p> <p>11 to Page 2 of Exhibit 9.</p> <p>12 A. Yes.</p> <p>13 Q. There are four Chrome extension</p> <p>14 listed there.</p> <p>15 Do you see that?</p> <p>16 A. Yes.</p> <p>17 Q. Video Downloader for Facebook, Album</p> <p>18 and Photo Manager for Facebook, PDF Merge-PDF</p> <p>19 Files Merger, and Tex Cam-Web Cam Effects.</p> <p>20 Do you see that?</p> <p>21 A. Yes.</p> <p>22 Q. Was Unimania using these extensions</p>	<p style="text-align: right;">Page 156</p> <p>1 early June 2018; is that what you are saying?</p> <p>2 A. Yes. Just from the Google Chrome</p> <p>3 store.</p> <p>4 Q. Now, as we were just discussing, the</p> <p>5 AdGuard report says that the extensions used a</p> <p>6 static salt to anonymize a user's Facebook ID;</p> <p>7 is that correct?</p> <p>8 A. Yes. The rest -- the rest are</p> <p>9 complete lies.</p> <p>10 Q. And because of the AdGuard report,</p> <p>11 you changed the method that you used to</p> <p>12 anonymize the Facebook user ID; is that</p> <p>13 correct?</p> <p>14 A. Yes. It pointed a security weakness</p> <p>15 that we've fixed.</p> <p>16 Q. And when did you fix it?</p> <p>17 A. Somewhere, I think, in June 2016 --</p> <p>18 2018.</p> <p>19 Q. Did any of -- as of September 2020,</p> <p>20 did any of BrandTotal or Unimania's extensions</p> <p>21 or applications use a static salt to anonymize</p> <p>22 information?</p>
<p style="text-align: right;">Page 155</p> <p>1 to collect information as of May 2018?</p> <p>2 A. Yes.</p> <p>3 Q. And does Unimania still use those</p> <p>4 extensions to collect data today?</p> <p>5 A. No.</p> <p>6 Q. Did Unimania ever use those</p> <p>7 extensions to collect information between May</p> <p>8 of 2018 and today?</p> <p>9 A. No. They -- they were not taken</p> <p>10 down either end of May or early June, I think.</p> <p>11 Q. And when you say, "they were taken</p> <p>12 down," do you mean --</p> <p>13 A. Taken down by Google -- by Google's</p> <p>14 Chrome store.</p> <p>15 MR. HAUER: Oren, make sure -- make</p> <p>16 sure you let counsel finish his question.</p> <p>17 THE WITNESS: Sorry.</p> <p>18 BY MR. HOLTZBLATT:</p> <p>19 Q. So just to clarify, these -- these</p> <p>20 applications and extensions were taken down</p> <p>21 from the Google Play store and the Google</p> <p>22 Chrome store by Google at the end of May or</p>	<p style="text-align: right;">Page 157</p> <p>1 A. No.</p> <p>2 Q. You said that the rest of the</p> <p>3 AdGuard report is a complete lie.</p> <p>4 A. Yes. It talks about us collecting</p> <p>5 purchase data and web history, which is totally</p> <p>6 not true.</p> <p>7 Q. Okay. Is there anything else in the</p> <p>8 report that is a complete lie?</p> <p>9 A. Yes. It says browsing histories of</p> <p>10 millions of users. We've never collected from</p> <p>11 millions of users.</p> <p>12 Q. Is there anything else that --</p> <p>13 A. I'm -- I'm -- I'm reading it kind of</p> <p>14 fast, but it says it is a spiraled extension.</p> <p>15 It is not a spiral extension. What -- what</p> <p>16 else? The key -- the key thing that we took</p> <p>17 from this report is just -- the spiral</p> <p>18 developers, come on, do they really believe</p> <p>19 that hashing a numeric value with a static salt</p> <p>20 cannot be decoded. That is it.</p> <p>21 Q. Are there any other changes that you</p> <p>22 made in response to the AdGuard report?</p>

<p style="text-align: right;">Page 158</p> <p>1 A. No. What -- what do you mean by</p> <p>2 "changes"?</p> <p>3 Q. Are there any other changes that you</p> <p>4 made to your extensions or applications in</p> <p>5 response to the AdGuard report?</p> <p>6 A. No.</p> <p>7 Q. Are there any other changes you made</p> <p>8 to your privacy policy or your terms of service</p> <p>9 in response to the AdGuard report?</p> <p>10 A. I don't think we did. At that -- at</p> <p>11 that kind of time frame, we were anyway</p> <p>12 changing to a new privacy policy and terms of</p> <p>13 use because of GDPR being applied at that same</p> <p>14 time frame.</p> <p>15 (Deposition Exhibit 10 was marked</p> <p>16 for identification.)</p> <p>17 BY MR. HOLTZBLATT:</p> <p>18 Q. I've just introduced -- I just put</p> <p>19 an identification marker on Exhibit 10.</p> <p>20 Can you see Exhibit 10?</p> <p>21 A. Yes, I see it.</p> <p>22 Q. Exhibit 10 is an e-mail from a Sagi</p>	<p style="text-align: right;">Page 160</p> <p>1 the -- the -- was the owner or in contract with</p> <p>2 third parties, and we -- Unimania had, like,</p> <p>3 active e-mails that people can contact us.</p> <p>4 Q. I understood from your earlier</p> <p>5 answer that you were hiding the relationship</p> <p>6 between Unimania and BrandTotal; is that</p> <p>7 correct?</p> <p>8 MR. HAUER: Object to the form.</p> <p>9 BY MR. HOLTZBLATT:</p> <p>10 Q. Were you hiding the relationship</p> <p>11 between Unimania and BrandTotal from your</p> <p>12 competitors?</p> <p>13 A. Yes.</p> <p>14 Q. And how were you hiding the</p> <p>15 relationship between Unimania and BrandTotal</p> <p>16 from your competitors?</p> <p>17 A. We -- we've created Unimania and the</p> <p>18 data collection assets were under the Unimania</p> <p>19 headline.</p> <p>20 Q. And does that mean that your</p> <p>21 competitors didn't know that the information</p> <p>22 that Unimania was collecting was going to</p>
<p style="text-align: right;">Page 159</p> <p>1 Katz at BrandTotal to Alon Leibovich, and you</p> <p>2 are CC'd on the e-mail. It's dated June 27,</p> <p>3 2018, correct?</p> <p>4 A. Yes.</p> <p>5 Q. Are you familiar with this e-mail?</p> <p>6 A. Yes.</p> <p>7 Q. And you received this e-mail?</p> <p>8 A. Yes, I did.</p> <p>9 Q. In the third paragraph of Exhibit 10</p> <p>10 Sagi Katz says that hiding the true identify of</p> <p>11 Unimania is triggering suspicion and lack of</p> <p>12 trust especially in these difficult times.</p> <p>13 Were you hiding the true identity of</p> <p>14 Unimania at the time?</p> <p>15 A. Yes. We were hiding it especially</p> <p>16 from competitor companies to BrandTotal,</p> <p>17 meaning that we didn't want other competitors</p> <p>18 to understand how we collect panel data.</p> <p>19 Q. And so were you also hiding the true</p> <p>20 identity of Unimania from users of the</p> <p>21 extensions?</p> <p>22 A. No. Unimania is the -- the --</p>	<p style="text-align: right;">Page 161</p> <p>1 BrandTotal?</p> <p>2 A. Yes.</p> <p>3 Q. And so your users also didn't know</p> <p>4 that the information that Unimania was</p> <p>5 collecting was going to BrandTotal?</p> <p>6 A. Yes.</p> <p>7 Q. So in that sense, you were hiding</p> <p>8 the identity of Unimania from your users,</p> <p>9 correct?</p> <p>10 A. Yes.</p> <p>11 MR. HAUER: Object to form.</p> <p>12 BY MR. HOLTZBLATT:</p> <p>13 Q. Mr. Sagi Katz was saying that hiding</p> <p>14 the identify of Unimania triggered suspicion</p> <p>15 and lack of trust, correct?</p> <p>16 A. Yes.</p> <p>17 Q. Who -- who was or is Sagi Katz?</p> <p>18 A. He was the external consultant I</p> <p>19 mentioned before Ofir came aboard as a</p> <p>20 full-time product manager, and he helped us</p> <p>21 doing business development and -- and defining</p> <p>22 the earlier versions of different extensions</p>

<p style="text-align: right;">Page 162</p> <p>1 and apps.</p> <p>2 Q. He proposes that you do something</p> <p>3 different with respect to the relationship</p> <p>4 between Unimania and BrandTotal; is that</p> <p>5 correct?</p> <p>6 A. Yes, because what we got at the end</p> <p>7 of it was the AdGuard report, which was --</p> <p>8 like, it was bad for us, and we were wondering</p> <p>9 whether it's because the -- the -- the -- the</p> <p>10 AdGuard blogger, like, considered Unimania to</p> <p>11 be too much of fishy and not a real company.</p> <p>12 If he would have used a different contact us</p> <p>13 e-mails, he would get to us and we might have</p> <p>14 had a conversation with him, but he didn't even</p> <p>15 try to contact us. He saw Unimania. He saw</p> <p>16 that there is no Unimania website, and it was,</p> <p>17 my guess, enough for him to call it a</p> <p>18 spyware -- a malicious spyware.</p> <p>19 Q. So did you take steps to change</p> <p>20 something with respect to the relationship</p> <p>21 between Unimania and BrandTotal after the</p> <p>22 AdGuard report came out?</p>	<p style="text-align: right;">Page 164</p> <p>1 [REDACTED]</p> <p>2 [REDACTED]</p> <p>3 [REDACTED]</p> <p>4 [REDACTED]</p> <p>5 [REDACTED]</p> <p>6 [REDACTED]</p> <p>7 [REDACTED]</p> <p>8 [REDACTED]</p> <p>9 [REDACTED]</p> <p>10 [REDACTED]</p> <p>11 [REDACTED]</p> <p>12 [REDACTED]</p> <p>13 [REDACTED]</p> <p>14 [REDACTED]</p> <p>15 [REDACTED]</p> <p>16 [REDACTED]</p> <p>17 [REDACTED]</p> <p>18 [REDACTED]</p> <p>19 [REDACTED]</p> <p>20 [REDACTED]</p> <p>21 [REDACTED]</p> <p>22 [REDACTED]</p>
<p style="text-align: right;">Page 163</p> <p>1 [REDACTED]</p> <p>2 [REDACTED]</p> <p>3 [REDACTED]</p> <p>4 [REDACTED]</p> <p>5 [REDACTED]</p> <p>6 [REDACTED]</p> <p>7 [REDACTED]</p> <p>8 [REDACTED]</p> <p>9 [REDACTED]</p> <p>10 [REDACTED]</p> <p>11 [REDACTED]</p> <p>12 [REDACTED]</p> <p>13 [REDACTED]</p> <p>14 [REDACTED]</p> <p>15 [REDACTED]</p> <p>16 [REDACTED]</p> <p>17 [REDACTED]</p> <p>18 [REDACTED]</p> <p>19 [REDACTED]</p> <p>20 [REDACTED]</p> <p>21 [REDACTED]</p> <p>22 [REDACTED]</p>	<p style="text-align: right;">Page 165</p> <p>1 [REDACTED]</p> <p>2 [REDACTED]</p> <p>3 [REDACTED]</p> <p>4 [REDACTED]</p> <p>5 [REDACTED]</p> <p>6 [REDACTED]</p> <p>7 [REDACTED]</p> <p>8 [REDACTED]</p> <p>9 [REDACTED]</p> <p>10 [REDACTED]</p> <p>11 [REDACTED]</p> <p>12 [REDACTED]</p> <p>13 [REDACTED]</p> <p>14 [REDACTED]</p> <p>15 [REDACTED]</p> <p>16 [REDACTED]</p> <p>17 [REDACTED]</p> <p>18 [REDACTED]</p> <p>19 [REDACTED]</p> <p>20 [REDACTED]</p> <p>21 [REDACTED]</p> <p>22 [REDACTED]</p>

<p style="text-align: right;">Page 222</p> <p>1 THE WITNESS: It's more complicated</p> <p>2 than that because we are -- we -- we -- we use</p> <p>3 our panel and we give the advertiser a</p> <p>4 realistic view both for Facebook specifically,</p> <p>5 as we've picked up from the panel, and other</p> <p>6 social platform as well as a whole.</p> <p>7 BY MR. HOLTZBLATT:</p> <p>8 Q. The information that you've</p> <p>9 described yourself as needing on Exhibit 19 is</p> <p>10 information that would be available through the</p> <p>11 insight API for the advertiser itself, correct?</p> <p>12 A. Yes.</p> <p>13 Q. You just need the advertiser's</p> <p>14 permission, correct?</p> <p>15 A. Yes.</p> <p>16 Q. And the reason you can't get</p> <p>17 information about other advertisers is that you</p> <p>18 don't have their permission, correct?</p> <p>19 A. Yes.</p> <p>20 MR. HOLTZBLATT: Bonnie, should we</p> <p>21 go off the record?</p> <p>22 THE COURT REPORTER: No. I'm okay.</p>	<p style="text-align: right;">Page 224</p> <p>1 record. The time is 12:10 p.m.</p> <p>2 (Whereupon, the proceeding was</p> <p>3 concluded at 12:10 p.m.)</p> <p>4</p> <p>5</p> <p>6</p> <p>7</p> <p>8</p> <p>9</p> <p>10</p> <p>11</p> <p>12</p> <p>13</p> <p>14</p> <p>15</p> <p>16</p> <p>17</p> <p>18</p> <p>19</p> <p>20</p> <p>21</p> <p>22</p>
<p style="text-align: right;">Page 223</p> <p>1 I'll go on mute. I'll get her to be quiet. My</p> <p>2 husband walked by.</p> <p>3 MR. HOLTZBLATT: One moment. I have</p> <p>4 no further questions, Mr. Dor. Thank you for</p> <p>5 your time.</p> <p>6 THE WITNESS: Thank you.</p> <p>7 MR. HAUER: I don't anticipate</p> <p>8 having any questions, but could we just take a</p> <p>9 quick break?</p> <p>10 MR. HOLTZBLATT: Yes.</p> <p>11 MR. HAUER: Thank you.</p> <p>12 THE VIDEOGRAPHER: We are going off</p> <p>13 the record. The time is 12:03 p m.</p> <p>14 (Recess taken.)</p> <p>15 THE VIDEOGRAPHER: We are back on</p> <p>16 the record. The time is 12:10 p m.</p> <p>17 MR. HAUER: I have no questions for</p> <p>18 the witness. I just want to preserve the</p> <p>19 witness's ability to review and sign.</p> <p>20 MR. HOLTZBLATT: I'm fine with that.</p> <p>21 THE VIDEOGRAPHER: This marks the</p> <p>22 end of the deposition. We are going off the</p>	<p style="text-align: right;">Page 225</p> <p>1 CERTIFICATE OF NOTARY PUBLIC</p> <p>2 I, Bonnie L. Russo, the officer before</p> <p>3 whom the foregoing deposition was taken, do</p> <p>4 hereby certify that the witness whose testimony</p> <p>5 appears in the foregoing deposition was duly</p> <p>6 sworn by me; that the testimony of said witness</p> <p>7 was taken by me in shorthand and thereafter</p> <p>8 reduced to computerized transcription under my</p> <p>9 direction; that said deposition is a true</p> <p>10 record of the testimony given by said witness;</p> <p>11 that I am neither counsel for, related to, nor</p> <p>12 employed by any of the parties to the action in</p> <p>13 which this deposition was taken; and further,</p> <p>14 that I am not a relative or employee of any</p> <p>15 attorney or counsel employed by the parties</p> <p>16 hereto, nor financially or otherwise interested</p> <p>17 in the outcome of the action.</p> <p>18</p> <p>19 </p> <p>20 Notary Public in and for</p> <p>21 the District of Columbia</p> <p>22 My Commission Expires: August 14, 2025</p>

<p style="text-align: right;">Page 226</p> <p>1 Ryan Hauer, Esquire 2 ryan.hauer@huschblackwell.com 3 January 25, 2021 4 RE: Facebook v. Brandtotal, et al. 5 1/13/2021, Oren Dor (#4399998) 6 The above-referenced transcript is available for 7 review. 8 Within the applicable timeframe, the witness should 9 read the testimony to verify its accuracy. If there are 10 any changes, the witness should note those with the 11 reason, on the attached Errata Sheet. 12 The witness should sign the Acknowledgment of 13 Deponent and Errata and return to the deposing attorney. 14 Copies should be sent to all counsel, and to Veritext at 15 cs-midatlantic@veritext.com 16 17 Return completed errata within 30 days from 18 receipt of transcript. 19 If the witness fails to do so within the time 20 allotted, the transcript may be used as if signed. 21 22 Yours, 23 Veritext Legal Solutions 24 25</p>	<p style="text-align: right;">Page 228</p> <p>1 Facebook v. Brandtotal, et al. 2 Oren Dor (#4399998) 3 ACKNOWLEDGEMENT OF DEPONENT 4 I, Oren Dor, do hereby declare that I 5 have read the foregoing transcript, I have made any 6 corrections, additions, or changes I deemed necessary as 7 noted above to be appended hereto, and that the same is 8 a true, correct and complete transcript of the testimony 9 given by me. 10 11 _____ 12 Oren Dor Date 13 *If notary is required 14 SUBSCRIBED AND SWORN TO BEFORE ME THIS 15 _____ DAY OF _____, 20____. 16 17 18 _____ 19 NOTARY PUBLIC 20 21 22 23 24 25</p>
<p style="text-align: right;">Page 227</p> <p>1 Facebook v. Brandtotal, et al. 2 Oren Dor (#4399998) 3 E R R A T A S H E E T 4 PAGE____ LINE____ CHANGE_____ 5 _____ 6 REASON_____ 7 PAGE____ LINE____ CHANGE_____ 8 _____ 9 REASON_____ 10 PAGE____ LINE____ CHANGE_____ 11 _____ 12 REASON_____ 13 PAGE____ LINE____ CHANGE_____ 14 _____ 15 REASON_____ 16 PAGE____ LINE____ CHANGE_____ 17 _____ 18 REASON_____ 19 PAGE____ LINE____ CHANGE_____ 20 _____ 21 REASON_____ 22 _____ 23 _____ 24 Oren Dor Date 25</p>	

EXHIBIT 2

REDACTED VERSION
OF EXHIBIT FILED
UNDER SEAL



Deposition of:

Yair Regev

November 18, 2021

In the Matter of:

Facebook v. BrandTotal

Veritext Legal Solutions

800-734-5292 | calendar-dmv@veritext.com |

Page 1

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
San Francisco Division

- - - - -x
FACEBOOK, INC., a Delaware :
corporation, :
:
Plaintiff/Counterclaim :
Defendant, :
:
Case No. :
v. :
:
3:20-cv-07182-JCS :
BRANDTOTAL, LTD., an Israel :
corporation, and UNIMANIA, :
INC., a Delaware corporation, :
:
Defendants/Counterclaim :
Plaintiffs. :
- - - - -x

Thursday, November 18 2021

Highly Confidential
Attorneys' Eyes Only
* Containing Source Code *

REMOTE ZOOM VIDEO deposition of YAIR REGEV, beginning at
8:01 a.m. EST, before Christina S. Hotsko, RPR, CRR, when
were present on behalf of the respective parties:

114

[illegible][illegible][illegible][illegible]

[illegible][illegible]

[illegible][illegible]

[illegible]

114

[illegible][illegible][illegible][illegible]

[illegible]

Category	Percentage
1. ...	~1%
2. ...	~100%
3. ...	~100%
4. ...	~100%
5. ...	~100%
6. ...	~100%
7. ...	~100%
8. ...	~100%
9. ...	~100%
10. ...	~100%
11. ...	~100%
12. ...	~100%
13. ...	~100%
14. ...	~100%
15. ...	~100%
16. ...	~100%
17. ...	~100%
18. ...	~100%
19. ...	~100%
20. ...	~100%
21. ...	~100%
22. ...	~100%
23. ...	~100%
24. ...	~100%
25. ...	~100%
26. ...	~100%
27. ...	~100%
28. ...	~100%
29. ...	~100%
30. ...	~100%
31. ...	~100%
32. ...	~100%
33. ...	~100%
34. ...	~100%
35. ...	~100%
36. ...	~100%
37. ...	~100%
38. ...	~100%
39. ...	~100%
40. ...	~100%
41. ...	~100%
42. ...	~100%
43. ...	~100%
44. ...	~100%
45. ...	~100%
46. ...	~100%
47. ...	~100%
48. ...	~100%
49. ...	~100%
50. ...	~100%
51. ...	~100%
52. ...	~100%
53. ...	~100%
54. ...	~100%
55. ...	~100%
56. ...	~100%
57. ...	~100%
58. ...	~100%
59. ...	~100%
60. ...	~100%
61. ...	~100%
62. ...	~100%
63. ...	~100%
64. ...	~100%
65. ...	~100%
66. ...	~100%
67. ...	~100%
68. ...	~100%
69. ...	~100%
70. ...	~100%
71. ...	~100%
72. ...	~100%
73. ...	~100%
74. ...	~100%
75. ...	~100%
76. ...	~100%
77. ...	~100%
78. ...	~100%
79. ...	~100%
80. ...	~100%
81. ...	~100%
82. ...	~100%
83. ...	~100%
84. ...	~100%
85. ...	~100%
86. ...	~100%
87. ...	~100%
88. ...	~100%
89. ...	~100%
90. ...	~100%
91. ...	~100%
92. ...	~100%
93. ...	~100%
94. ...	~100%
95. ...	~100%
96. ...	~100%
97. ...	~100%
98. ...	~100%
99. ...	~100%
100. ...	~100%

[illegible][illegible]

[illegible][illegible][illegible][illegible]

[illegible]

██████████

1

59 (Pages 230 - 233)

114

[illegible]

Page 302

C E R T I F I C A T E

I do hereby certify that the aforesaid
testimony was taken before me, pursuant to
notice, at the time and place indicated; that
said deponent was by me duly sworn to tell the
truth, the whole truth, and nothing but the
truth; that the testimony of said witness was
taken by me in stenotypy and thereafter reduced
to typewriting under my direction; that said
statement is a true record of the proceedings;
that I am neither counsel for, related to, nor
employed by any of the parties to the action in
which this statement was taken; and, further,
that I am not a relative or employee of any
counsel or attorney employed by the parties
hereto, nor financially or otherwise interested
in the outcome of this action.



CHRISTINA S. HOTSKO, RPR, CRR

77 (Page 302)

EXHIBIT 3

SEPTEMBER 2019

CHARTING A WAY FORWARD

Data Portability and Privacy

Erin Egan

VICE PRESIDENT AND
CHIEF PRIVACY OFFICER, POLICY

FACEBOOK

Table of Contents

03	I. Intro
06	II. The Challenge
09	III. Five Questions About Portability and Responsibility
09	QUESTION 1
	What is “data portability”?
13	QUESTION 2
	Which data should be portable?
14	QUESTION 3
	Whose data should be portable?
15	QUESTION 4
	How should we protect privacy while enabling portability?
20	QUESTION 5
	After people’s data is transferred, who is responsible if the data is misused or otherwise improperly protected?
24	IV. What’s Next?
25	End Notes

Data Portability and Privacy

There's growing agreement among policymakers around the world that data portability—the principle that you should be able to take the data you share with one service and move it to another—can help promote competition online and encourage the emergence of new services. Competition and data protection experts agree that, although there are complicated issues involved, portability helps people control their data and can make it easier for them to choose among online service providers.

The benefits of data portability to people and markets are clear, which is why our CEO, Mark Zuckerberg, recently called for laws that guarantee portability.¹ But to build portability tools people can trust and use effectively, we should develop clear rules about what kinds of data should be portable and who is responsible for protecting that data as it moves to different providers.² The purpose of this paper is to advance the conversation about what those rules should be.

We hope this paper will anchor a series of conversations among stakeholders around the globe about how to build portability products in a privacy-protective way while also helping keep competition vibrant among online services. At the conclusion of the series, we hope to have a portability framework that will improve our own and others' product development efforts, guide industry collaboration and potentially inform future legislation.

To that end, the paper sets out five questions about privacy and portability:

01 What is “data portability”?

Should all user-directed data transfers to third parties be considered “data portability”?

02 Which data should be portable?

Should portable data be limited to only the data a person has provided to the service provider (and what does it mean to “provide” data)?

03 Whose data should be portable?

If data is associated with more than one person—a common scenario for social networking services—should transferring providers limit data portability? How can providers ensure that each individual's rights are accounted for?

04 How should we protect privacy while enabling portability?

What responsibilities, if any, should transferring providers have with respect to (1) requesting users, (2) others whose interests may be implicated by a transfer, and (3) potential recipients of the data?

05 After people's data is transferred, who is responsible if the data is misused or otherwise improperly protected?

How should responsibility be allocated as between the transferring and recipient providers? Should users themselves be responsible for issues that affect their (or their friends') data?

We're fortunate to already have perspectives of key stakeholders on these questions, such as the EU data protection authorities' 2017 guidance on the right to data portability in the context of the European Union's General Data Protection Regulation (“GDPR”); two recent papers from Singapore's Personal Data Protection Commission; a report on competition policy in the digital era commissioned by the European Commission's Directorate-General for Competition; and a report on data mobility commissioned by the UK's Department for Digital, Culture, Media & Sport. But we believe the industry would benefit from additional discussion and guidance.

Importantly, this paper focuses on data portability as an action that individual users of a service choose to take; it does not focus on business-to-business transfers of information. We recognize that the latter transfers can be important to choice and competition, as well. That's why we're looking into ways to make data available to other companies that can, for example, help them train artificial intelligence models.

The privacy issues implicated by these kinds of transfers are different from those that arise when individuals choose to transfer their data. In this paper, we focus on transfers initiated by individuals, but we're continuing to engage with experts as we look into other types of transfers, as well.

Thank you in advance for participating in this crucial conversation. We welcome feedback from all stakeholders, and we look forward to hearing your thoughts.

The Challenge

One of our core privacy principles at Facebook is that we enable people to control the use of their information on our services.³ Guided by that principle, we have built tools such as the controls that allow people to select the audience for their profile information and their posts, as well as Ad Preferences, which helps people control how their information is used to show them ads.

These tools help people control how their information is used on Facebook. But we also understand that giving people control means facilitating choice and competition by empowering them to move their information to a different service altogether—that we should, in other words, build products that enable data portability.

Data portability recently became a legal requirement in certain places through laws such as the GDPR⁴ and the California Consumer Privacy Act (“CCPA”).⁵ but Facebook has been considering ways to improve people’s ability to transfer their Facebook data to other platforms and services for some time. For example, since 2010, we’ve offered Download Your Information (“DYI”), which is designed to help people access and share their information with other online services. In connection with the GDPR coming into force, we made DYI better suited for portability by enabling people to receive their information in the commonly used structured JSON format.

Although DYI is a robust data portability tool, we believe we can go further and improve choice and control by making it even easier for people to export their data to other services. In his recent op-ed, Mark Zuckerberg wrote that “[t]rue data portability should look more like the way people use our platform to sign into an app

than the existing ways you can download an archive of your information.”⁶ In other words, people should be able to transfer their information directly to a provider of their choosing, in a way similar to how people use Facebook Login today.

To help achieve this goal, we’ve joined Google, Microsoft, Twitter, Apple, and others in the Data Transfer Project, an open-source software project designed to help participants develop interoperable systems that allow individuals to transfer their data seamlessly between online service providers.⁷ This project was inspired in part by the GDPR’s right to portability, but we believe data portability will soon become the norm in other regions of the world. For example, California’s new data portability provision will become effective in 2020; governments in Singapore, Australia, India, Hong Kong, and elsewhere may also soon pass laws supporting portability; and the European Commission is considering portability in the context of competition policy for the digital age.⁸

Proponents of portability recognize that, in order to succeed, industry needs to address potential fundamental privacy questions, such as those we pose in this paper.⁹ But there has not been detailed guidance with respect to how service providers could or should balance the benefits to personal autonomy, innovation, and competition from portability against the potential risks to privacy and security.¹⁰ For example, the EU’s Article 29 Working Party (succeeded by the European Data Protection Board, which adopted its guidance) has recognized the risks to security posed by data portability tools—but has stated only that security measures should not “obstruct” people from exercising portability rights.¹¹ Similarly, the Working Party noted the importance of limiting a person’s right to portability where its exercise could harm other people, but provided no specific guidance on how or when to implement this limitation.¹²

Download Your Information

You can download a copy of your Facebook information at any time. You can download all of it at once, or you can select only the types of information and date ranges you want. You can choose to receive your information in an HTML format that is easy to view, or a JSON format, which could allow another service to more easily import it.

Downloading your information is a password-protected process that only you will have access to. Once you've created a file, it will be available for download for a few days.

If you'd like to view your information without downloading it, you can [Access Your Information](#) at any time.

New File Available Files

Date Range: All of my data ▼ Format: JSON ▼ Media Quality: Medium ▼ **Create File**

Your Information ⓘ Download All

	Posts Posts you've shared on Facebook, posts that are hidden from your timeline, and posts you have created	<input checked="" type="checkbox"/>
	Photos and Videos Photos and videos you've uploaded and shared	<input checked="" type="checkbox"/>
	Comments Comments you've posted on your own posts, on other people's posts or in groups you belong to	<input checked="" type="checkbox"/>
	Likes and Reactions	<input type="checkbox"/>

In addition, some guidance on portability seems at odds with other guidance on companies' responsibilities for protecting against data misuse by third parties to which companies enable data transfers. Privacy regulators have made it clear that, at least in the context of some third-party relationships, platforms like ours should have protections in place that account for the privacy risks that can arise from transfers.¹³ But with respect to the GDPR's right to portability, the Working Party both endorses the idea of enabling people to disclose their data to third parties¹⁴ and states that "the data controller is not responsible for compliance of the receiving data controller with data protection law, considering that it is not the sending data controller that chooses the recipient."¹⁵

Several reports on competition in digital markets have emphasized the value of portability for innovation, and have noted that we need to address potential privacy and security risks. For instance, the report of the UK's Digital Competition Expert Panel stated that "[a]ny approach to support this form of data sharing will also have to ensure that robust privacy safeguards are adopted to respect the privacy rights and expectations of users."¹⁶ But the report does not expand on what those safeguards should be.

As we move toward a world of greater portability, we and other companies would benefit from clear rules that help resolve these kinds of questions—questions about portability, privacy and responsibility.

Five Questions About Portability and Responsibility

As discussed above, data portability helps people control their data and choose the services that best meet their needs. At the same time, portability can present challenges to safeguarding privacy interests. To address these challenges, we're seeking feedback and guidance from a wide range of stakeholders about how to build portability in a way that empowers people and fosters competition while maintaining their trust in online services.¹⁷ In this section, we set out five key questions, the answers to which will help build the next generation of portability products. We also offer some thoughts on how to answer these questions to help further the conversation on these important topics.

QUESTION 1

What is “Data Portability”?

Based on some of the sources that discuss data portability, one might assume that it's a straightforward concept with a settled meaning. For example, the Article 29 Working Party explained that, in the GDPR context, portability is simply the right to receive personal data and transmit it from one service provider to another.¹⁸ The International Organization for Standardization defines “data portability” as the “ability to easily transfer data from one system to another without being required to re-enter data,” focusing on the ease with which data can be moved.¹⁹

But when we move beyond esoteric discussions of portability, we find that there's considerable variation in people's views. In fact, we've heard calls—sometimes from the same stakeholder—both to enable greater data portability and to limit people's

ability to share their data with third parties.²⁰ The context in which we typically hear the latter is in connection with our consumer app platform (or “Platform” for short), which, among other things, refers to the set of technologies we make available for developers that want to enable people to (1) share their Facebook information with the developer’s app or (2) send information from the developer’s app to Facebook. The best-known Platform tool is Facebook Login, which enables people to log in to—and share their information with—third-party apps.

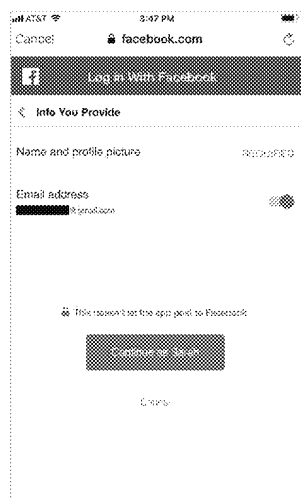
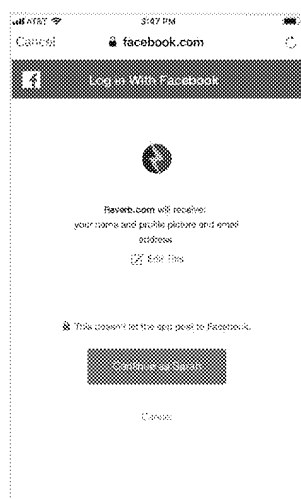
Particularly following the Cambridge Analytica matter, we’ve consistently heard calls from various stakeholders to limit the information that apps can receive through Facebook Login and to enhance our oversight of the apps that do receive that information.²¹ These calls suggest that some commentators may view the platform-to-app transfers of data as different from transfers made possible by “true” data portability. For example, Facebook’s 2019 Consent Order with the FTC treats portability transfers separately from other transfers.²²

By contrast, other commentators have suggested that Cambridge Analytica happened because of data portability, implying that platforms like ours (as well as iOS, Android, Twitter, and others) were already engaging in data portability when we enabled people to share their data with apps on Platform.²³

The question that comes out of these conversations is: When is a person’s request to transfer data a *portability* request? The answer is crucial, not least because of the legal rights that attach to portability requests. Under the GDPR, for example, portability requests must be fulfilled “without hindrance,” raising questions about

whether there are any circumstances in which a service provider may deny a request, limit the data available in response to the request, or restrict the third party’s ability to use the data following the transfer. It’s clear that many stakeholders believe platforms should impose data-use restrictions on recipients of user data, but the question remains whether service providers must make alternative mechanisms available to enable transfers without such restrictions. If so, how are these two transfers different from each other?

To begin to answer this question, it is important to recognize that most user-directed transfers of data to third parties look and operate similarly. Transfers generally involve three parties: requesting users, transferring entities, and recipient entities.²⁴

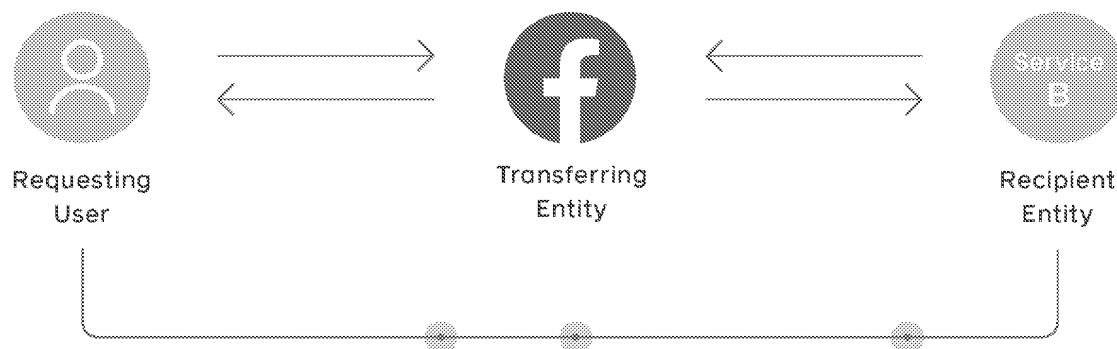


From a technical perspective, a data transfer begins when the requesting person instructs the transferring entity to export his or her data. The transferring entity then sends the requested data either to the requesting person (who then may use the data or send it to the recipient entity) or directly to the recipient entity. Once the data is shared with the recipient entity, the user can then interact with the data on or through that service.

But transfers that look similar technically may work differently in practice. One factor that differentiates transfers is the relationship between the transferring entity and the recipient entity and the rules, if any, that govern transfers between them. In general, these user-directed transfers of data to third parties can be thought of as occurring on a spectrum, with progressively more restrictions imposed as the relationship between the transferring entity and recipient entity grows closer (setting aside, for the moment, what the scope of the data transferred should be, which we discuss later in the paper). Three broad categories of user-directed transfers could be described as follows:

1. OPEN TRANSFERS

Requesting users can receive their data and transfer it to any recipient entity without controls or limitations (beyond those that exist under law) imposed on the recipient by the transferring entity. In this model, either the users can perform the transfer to a recipient via their own device (as in our DYI tool) or the transferring entity can facilitate a direct transfer. Apart from the technical connection made for the purpose of enabling a transfer, there is no relationship between the transferring and recipient entities. This model seems closest to that anticipated by the GDPR and the Working Party guidance.



2. CONDITIONED TRANSFERS

Requesting users can receive their data and transfer it to any recipient that has met certain conditions imposed by the transferor. The relationship between the transferring and recipient entities only exists for the purpose of enabling such user requests; there is no ongoing relationship. As we examine below, this could be a way to think about user requests to port data directly between services, the technical means for which the Data Transfer Project is working toward.



3. PARTNERSHIP TRANSFERS

Requesting users can receive their data and transfer it to a recipient with which the transferor has an ongoing relationship regarding such transfers, the terms of which may include provisions on how the recipient may use the data obtained in the transfer. Here, the relationship between the transferring and recipient entities exists for a purpose beyond simply effectuating users' transfer requests—such as, for example, integrating one of the entities' features into the other entity's products. Transfers through the Facebook Platform are an example of partnership transfers.

When thinking about portability, it helps to acknowledge the differences between these categories of user-directed data transfers. The question we need to answer is which transfers should be considered as involving "data portability" and what obligations on each party in the transaction, if any, should flow from each model? Open transfers seem to be clearly consistent with the nature of data portability as described in the GDPR and elsewhere, but what about conditioned transfers, in which the transferring entity may choose to limit the third parties to which the user may send data? Are such limitations consistent with the right to portability? Should partnership transfers—like the transfers from Platform—ever be viewed as involving data portability?

In our conversations with stakeholders so far, the general view about these questions has been that a transferring entity may—and should—impose some

baseline privacy and data protection restrictions around transfers even when carrying out the transfer to comply with a portability request. But, as discussed below, questions remain about what kinds of conditions are appropriate. Restrictions along the lines of those we impose through Platform strike some as too restrictive to be consistent with portability. Our recent settlement with the FTC suggests that some regulators may view Platform-style transfers as distinct from portability transfers.²⁵ Where the line is between these two categories will likely be the line between portability and other data transfers.

QUESTION 2

Which Data Should be Portable?

A primary purpose of enabling data portability is to provide individuals with control over their data. But what exactly is “their data”? It seems clear that people should be able to transfer data such as the photos they upload to a service or the posts they make to a social network. It’s less clear what other data should be included.

Should people be able to export the information that a service provider receives as they use its features—information like search history, location data, and activity logs? What about information generated about people by the service provider on the basis of people’s uploaded data or their interactions with the service, like the inferences used to personalize music, events, and ads, or to identify potentially fraudulent activity?

The GDPR and the Working Party guidance suggest that there should be limits around the data that is subject to the portability right. The GDPR requires portability of personal data that a person has “provided to” a data controller.²⁶ The Working Party has suggested that people be able to transfer personal data that they actively provide to a service provider or that the service provider observes about them as they use its services, but not data that the service provider infers about them based on that use.²⁷

Another question—particularly when it comes to data about a person’s use of a service—is how service providers’ retention of data might bear on the question of which data should be portable. It seems uncontroversial that service providers should not be required to retain data solely for the purpose of enabling portability, so at least some data won’t be portable simply because it won’t be available at the time of the request. But what about the data that is technically available but will soon be deleted? Should a service provider build tools to export this data too?

Still another question is whether there are cases in which the burden of making data portable outweighs the person’s interest in exporting it. For example, a service’s data about a person’s use of a service could include a list of every page

or piece of content the person has viewed within a certain period, every link he or she has clicked on, and every notification he or she has received. Service providers often keep logs of this information for periods of time, but the process of making this log data portable could be challenging, and the benefits to the user might not always be obvious. Would it be useful, for example, to be able to export a list of all the links you've clicked on Facebook within a certain period? Or an archive of every ad you've seen while scrolling through News Feed?

Given that portability is partly intended to encourage competition and the emergence of new services, we should consider these questions in light of the operational burden they would impose on service providers with fewer resources than companies like Facebook. Viewed from that angle, it seems clear that some limitations should be imposed around a service provider's obligation to make observed data portable. Considering data retention periods and weighing the burden on providers against the benefit to users could be helpful in determining what those limitations should be or to whom they should apply.³⁸ But we will need to answer questions about how any balancing should be conducted—and by whom.

QUESTION 3

Whose Data Should be Portable?

Providing data portability helps people exercise control over their data. But what happens when one person wants to transfer data that is associated with another person? What if, for example, Person A wants to move her photos from one service to another, but those photos include images of Person B? What are Person B's rights to control his information in that scenario? What if people want to export the contents of their phone's address book or a list of their contacts' birthdays to a new service? Should a person's contacts—whose information would be shared with the new service—have a say in whether the person may share the information?

As these examples illustrate, it is sometimes difficult to delineate whose data should be transferred in response to a data portability request.³⁹ We've found this to be particularly true for Facebook, a core function of which is to allow users to connect with other people and create shared experiences. And the ability to transfer data about your contacts—or friends—can raise especially challenging privacy issues.⁴⁰

Some have suggested that the only data that should be transferred following a portability request should be the data that the requesting person "owns."⁴¹ If the requesting users own the data they provide to a service, the argument goes, then they should be able to do whatever they wish with it, including porting it to another entity. Conversely, if requesting users do not own some of the data they wish to transfer, then they should not be able to port that data.

The concept of data as property has been viewed by some as controversial and may lead to *more* questions that stretch well beyond the portability context.³² For example, in practice, many types of information have more than one owner. If you have my phone number in your address book, for example, are you the owner of that phone number? Moreover, in the EU, data protection (as a fundamental right) does not vary depending on who, if anyone, “owns” the data in question.³³

Another approach to deciding whose data should be made portable in response to a request could be based on factors such as who provided the data, whether the service provider has associated it with a particular user, and the sensitivity of the data. Consider the following scenario:

Person A uploads a video of herself and three of her friends (Persons B, C, and D). She doesn’t take any steps that would enable the service to identify her friends (such as “tagging” them). At first glance, it seems clear that Person A should have the right to port the video to a new service, but what rights, if any, should Persons B, C, and D have with respect to the video? And who is best positioned (as between Person A and the service provider) to address those rights?

Now consider a slightly different version of the same scenario: Person A uploads the video, but this time, she tags Persons B, C, and D, who all happen to be users of the service. In this scenario, the service provider may be in a position to inform Persons B, C, and D about a portability request. Assuming this happens, should they have the right to stop Person A from transferring the video?

How might the answers change if, instead of a video, we were talking about email addresses in Person A’s contacts list? Should it be easier or harder for Person A to port them than to port Person A’s photos? What about emails themselves, which a person might want to export to a new email service (e.g., from Gmail to Outlook)?

We think a multifactor approach that considers questions like these and the factors above is likely preferable to an approach that focuses on data ownership. But *how we weigh these factors* in the analysis of whose data should be portable requires much more discussion and guidance.³⁴

Commentators often describe the question of whose data should be transferred in connection with portability as having to do with the portability of a person’s “social graph”—the map of the connections between a user and other users and entities on that service. Some advocates of data portability have argued that services like ours must enable people to transfer their own data as well as data about their social

graph, in part because the latter data may help enable other social networking companies to innovate.³⁵ Without a portable social graph, these advocates argue, users may not be able to seamlessly transfer into alternative social networks.

We think there are strong arguments on both sides: Enabling portability of the social graph can be important for innovation and competition, but doing so also comes with important privacy questions. The key question is whether we can find ways to enable this sharing that protect the privacy of all individuals involved. We turn to this issue in the next section.

QUESTION 4

How Should We Protect Privacy While Enabling Portability?

Questions 1 through 3 involve questions about circumstances before people choose to port their data. Once we know (1) that we're dealing with a user-directed transfer of data, (2) which types of data should be transferred, and (3) whose data should be transferred, we next need to ask how we can enable portability while protecting privacy.

Although we're seeing laws that require data transfers—including data portability laws—there is little guidance around protecting privacy in connection with those transfers. Stakeholders have raised concerns about the privacy and security risks of portability tools, and about the lack of clarity from policymakers and regulators about what is expected of transferring entities.³⁶

More clarity on these points is key because in order for data portability to enhance people's control over their data, users should be able to trust that their data will be handled responsibly during and after the transfer. We've found it helpful to think through these questions about privacy and portability by considering transferring entities' actions with respect to (1) requesting users, (2) non-requesting users whose data would be transferred, and (3) recipient entities.

REQUESTING USERS

Given that portability is about helping people stay in control of their data, it seems clear that transferring entities should focus on making sure that requesting users can make informed choices about transferring their data. This means ensuring that requesting users have information about the entity to which they want their data to be transferred. But exactly what kind of information a person should have—and how it should be made available (and by whom)—are questions that haven't been fully answered by policymakers, regulators, or other stakeholders.

In its assessment of portability under the GDPR, the Working Party explained that although people are “responsible” for “identifying the right measures in order to secure personal data” with the entity to which they’ll transfer their data, the transferring entity should make the data subject “aware” of measures to enable the person to take appropriate steps.³⁷

Compare that guidance with a recent discussion paper from Singapore’s Personal Data Protection Commission, which suggests that transferring entities should go further, including by providing information such as how user data will be used by the data recipient; the nature of the new product or service that the user is acquiring; and the track record, reputation, and data management and protection practices of the data recipient.³⁸ In its May 2019 consultation paper on the topic, the Commission further proposed requiring organizations to provide relevant information to people as part of a binding code of practice.³⁹

These perspectives are helpful starting points, but we think there’s more to discuss about what, if any, information should be provided to people who want to transfer their data—as well as how, and by whom, that information could be presented in a helpful way.

NON-REQUESTING USERS

Some data portability requests may involve data associated with people other than the person making the portability request (“non-requesting users”). As discussed above, there are tough questions about whether these users’ data should be transferred at all. If it should, service providers will need to account for the privacy interests of these users.

Some stakeholders have proposed consent mechanisms or similar means of allowing people to grant each other permission to have their data exported from a particular service—that is, for User A to be able to grant User B the permission to share User A’s data with a recipient entity.⁴⁰ Given the focus on consent as part of a potential solution to the concern over the porting of non-requesting users’ data, we want to explore whether—and, if so, how—services could offer meaningful choice and control to non-requesting users. Would requiring consent inappropriately restrict portability? If not, how could consent be obtained? Should, for example, non-requesting users have the ability to choose whether their data is exported each time one of their friends wants to share it with an app? Would such an approach lead to notice fatigue?⁴¹ For users of a particular service, would it be better to give people a setting enabling them to always permit their friends (or other contacts) to transfer all—or certain categories—of their personal data to third parties? And how could we address non-users whose information is shared on a particular service?

A. Portability of Social Graph Data

As discussed above, some stakeholders view the transfer of social graph information (such as contacts lists) as an important way to help emerging social networking companies innovate and develop new services.⁴² There has been considerable discussion, and some concrete proposals, about ways to enable the export of this kind of information. Among these proposals, enabling the export of cryptographically obscured (or “hashed”) versions of users’ and their contacts’ unique user identifiers has been described as “[p]erhaps the most promising avenue for social graph portability.”⁴³

This solution aims to hide user IDs (e.g., email addresses) from the recipient entity while still providing some ability to reconstruct the transferring users’ social graph, potentially helping address the privacy challenges of sharing friends’ data with third parties by avoiding unnecessary exposure of personal data. However, experts have noted that this proposal would “require a major collaborative technical effort that could raise unanticipated privacy and security challenges as well as legal compliance questions[.]”⁴⁴ Below, we explore two commonly discussed approaches to sharing hashed contacts’ data and the potential challenges such approaches could raise.

First, a provider could share a list of hashed identifiers that are associated with the requesting user and their contacts. The simplest way of doing this is to share hashed versions of a contact’s name (which is not necessarily unique) or email address. If Users A and B are both connected to User C, and both share their hashed contacts’ lists with a service, then that service will know that User A and User B are both connected to User C, but it cannot learn additional information about User C unless User C has also ported his or her personal data to the same service.

Another option is to share identifiers not associated with users but rather with relationships between users. In this system, if Users A and B are both friends with User C, and both share their contacts lists, then—unlike above—the recipient service cannot know that Users A and B are both friends with User C. This is because the identifier for the relationship between Users A and C is different from the identifier for the relationship between Users B and C. However, if User C chooses to also share their contacts list, then User C will share the same two identifiers for their relationship with Users A and B respectively, at which point the receiving service can match up these identifiers to know that User C is connected to User A and User B.

Both of these approaches have drawbacks that require further discussion with stakeholders. In the first approach, it may be possible for the recipient to infer information about User C based solely on their relationship with Users A and B. For example, if Users A and B share an employer or are members of the same political party, then the recipient may be able to infer those facts about User C and

determine User C's identity with minimal additional information. The second approach doesn't suffer from this issue, but its utility to the recipient may be more limited because a relationship is only recognizable by the recipient service if both contacts choose to share their information with the recipient service.

Another challenge for social graph sharing is to settle upon a common data model that is specific enough to be useful but broad enough to apply across services. For example, some social networks have a single account per user, while others allow multiple accounts for one user. If User A is connected with one of User B's accounts but not with another, how should this relationship be reflected when either user shares a contacts list with a service that permits only a single account per user? Further risk of data leakage is introduced when users who port contacts data from a pseudonymous social network to one that requires real names. Recipients (or even the requesting user) may be able to infer the actual identities of pseudonymous users based on commonalities with their known contacts.

Moreover, social graph sharing can grow more complex as we consider additional layers of social interaction. For example, if one of User A's posts is ported to another social network and User B has commented on or liked that post, when should that comment be visible, who should be able to see it, and how should User B be identified, if at all, on the new service? The answers to those questions could vary based not only on the audience controls at the new service, but also on the mechanism used to port and identify contacts at the new service.

POTENTIAL RECIPIENTS OF PERSONAL DATA

Over the past year, we have heard calls from many stakeholders that service providers should make additional efforts to protect against data misuse by at least certain third parties.⁴⁵ But what should those efforts consist of when it comes to portability?

There is little expert commentary on this question. In the GDPR context, the Working Party's guidelines state only that a transferring data controller "is responsible for taking all the security measures needed to ensure . . . that personal data is securely transmitted (by the use of end-to-end or data encryption) to the right destination (by the use of strong authentication measures)."⁴⁶ The guidelines suggest risk mitigation measures, such as using additional authentication information, or suspending or freezing transmission if there is suspicion that an account has been compromised. However, these security measures "must not be obstructive in nature and must not prevent users from exercising their rights[.]"⁴⁷

Apart from these basic steps, the Working Party does not offer guidance on how service providers should protect against misuse by third parties. In conversations with stakeholders, we often hear that transferring service providers should consider

imposing additional controls to ensure that recipients process user data with privacy and security in mind. For instance, providers could require recipients to certify (1) the purposes and uses for the personal data they may receive pursuant to a data portability request, and (2) that they are processing data in accordance with applicable laws and data protection requirements. We also hear that providers should even consider monitoring recipient entities' processing of data and enforcing against recipient organizations who fail to process data according to applicable laws and data protection requirements, an extremely challenging (if not impossible) requirement and one that seems not to be required under the GDPR formulation of portability.

At the same time, we hear concerns that these kinds of requirements may be inconsistent with "true" portability: If people want to transfer their data to a particular entity, what business is it of the transferring entity to assess the purposes for which the person's data will be processed or whether the recipient complies with the law? What if the transferring entity and the recipient disagree about what the law requires? Should the transferring entity get to decide? There may be a point at which the transferring entity's efforts to exercise diligence beyond securing the transfer may impose undue friction on the abilities of users to switch to competing services.

One proposed response to such concerns is an accreditation system.⁴⁸ Under an accreditation model, potential recipients of user data could demonstrate, through certification to an independent body, that they meet the data protection and processing standards found in a particular regulation, such as the GDPR.⁴⁹ Accredited entities could then be identified with a seal and would be eligible to receive data from transferring service providers. The independent body (potentially in consultation with relevant regulators) could work to assess compliance of certifying entities, revoking accreditation where appropriate.

Another potential solution, which may be compelling to providers that operate in a country without a comprehensive data protection framework, could be the creation of a portability-focused code of conduct administered by an independent organization.⁵⁰ The code of conduct could require entities to implement privacy and security safeguards before receiving user-requested data. The independent organization could engage in monitoring and enforcement of its signatories for potential violations. A key question for this model would be how it should treat recipient entities that fail to comply with or don't sign on to the code. Even if the user's request to transfer information to such a recipient must be fulfilled, information about a recipient's noncompliance with (or refusal to sign on to) the code of conduct may still provide important information to users about the entity's privacy and security safeguards.

QUESTION 5

After people's data is transferred, who is responsible if the data is misused or otherwise improperly protected?

People and service providers need clarity on who is responsible for processing and protecting data before, during, and after a user-requested data transfer. Regulators have taken the position that platforms like Facebook may be responsible for ensuring that data is protected following certain user-requested transfers of data to third parties. Is that the case when it comes to data portability requests?

With respect to the exercise of the GDPR's portability right, the Working Party's guidelines provide a clear allocation of responsibility when a service provider ports data to another entity at a user's request.⁶¹ Responsibility and liability generally follow user data to its new destination. Before and during any data transfer, the transferring service provider is responsible for ensuring that they act on the requesting user's behalf, securing the transmission on its way to the correct recipient, and mitigating any risks associated with data portability. Recipients must ensure that they receive only data that is necessary and relevant to the service they are providing to the requesting user.

After the transfer, the transferring service provider is not responsible for the processing handled by the data subject or by another company receiving personal data (since they are only acting on behalf of the data subject and not choosing the recipient organization). Instead, according to the Working Party, responsibility vests in the recipient, which must now process and protect the personal data it accepts according to its obligations under the GDPR.

The Personal Data Protection Commission of Singapore's discussion paper also proposes a liability model, in which transferring entities would be exempted from claims for damage arising from misuse of data by the recipient—a result the Commission believes appropriate, given that transferors cannot feasibly vet all potential recipients. The paper also states that the transferor should not be liable for claims "relating to the accuracy and quality of the ported data unless it was demonstrated that the data was corrupted while under the care of the [transferor]."⁶² In its most recent consultation paper on the topic, the Commission does not mention liability but appears to limit post-transfer responsibilities for transferor entities to "check[ing] that the data transmitted has been received by the receiving organization and assist[ing] with any queries it may have with respect to the data transmitted."⁶³

But there are clearly some circumstances in which policymakers and regulators expect transferring entities to maintain responsibility even after the transfer. One

way to harmonize this reality with the Working Party's guidelines and the Personal Data Protection Commission's discussion paper may be to further clarify that service provider responsibility may vary depending on where on the spectrum a transfer falls—i.e., whether it is an open transfer, a conditioned transfer, or a partnership transfer, as discussed in Section II.A. For instance, should providers be deemed more accountable in a partnership transfer (e.g., a model like Facebook's Platform) due to the closer nature of their relationship with the recipient organization and a purpose for the transfer that extends beyond satisfying a request from a user?

For open transfers, perhaps the most a service provider should be responsible for is helping users take responsibility for the risks associated with taking their data to a new service; provided this has occurred, responsibility for protecting data would rest solely with the recipient. Service providers might explore tools to help users understand security risks and protocols for their downloaded data. Providers could also consider giving users guidance on how to inspect recipient organizations for potential abuse or insufficient security safeguards. For instance, providers could teach users ways to confirm the authenticity of the recipient organization (that it is what it says it is); check the website security for recipient organizations (e.g., the difference between HTTP and HTTPS); secure their devices when they download data (e.g., not using public Wi-Fi when downloading data); and identify whether the recipient organization has appropriate policies in place (e.g., checking privacy policies to determine whether an entity will sell user data that it receives).

For conditioned transfers, one approach would be for service providers to require recipients to certify that they're accredited by a standards body, in compliance with a relevant code of conduct, or otherwise that they will process personal data in accordance with applicable laws and data protection requirements before fulfilling a transfer request. Once providers have received such a certification, they could be relieved of responsibility (and liability) for data issues that arise after transfer.

For partnership transfers, it may be more appropriate to impose some degree of responsibility on the transferring entity, even for conduct that occurs after the transfer. To the extent feasible, some enhanced oversight of recipients' handling of people's data following a transfer may also be appropriate.

Finally, there is the complex question of responsibility when it comes to individuals about whom data is transferred by another party as part of a portability request. The Working Party guidelines note that if a user's data portability request involves personal data belonging to third parties, the requesting user is also responsible for the processing operations that the user initiated (to the extent that such processing is not decided by the controller), outside of an exemption for household or personal use.⁵⁶ Imposing responsibility (and liability) for requesting users who transfer contacts' data could chill interest in portability generally, and in social graph

portability specifically. Could a better outcome be to limit liability for requesting users to only cases involving truly unreasonable or reckless behavior, such as knowingly transferring their contacts' data to a party known to have a history of data misuse or poor data protection practices?

What's Next?

Data portability promises to give people unprecedented control of their information and to support continued vibrant innovation and competition online. The GDPR and other laws have prompted considerable investment in portability tools. This paper and the conversations that will follow it are intended to promote portability by laying out the issues and starting to address hard questions about how portability can be implemented in a privacy-protective way. We strongly believe that it can, and we look forward to collaborating with a range of stakeholders on solutions in the months to come.

END NOTES

Data Portability and Privacy: Charting a Way Forward

1. See Mark Zuckerberg, *The Internet Needs New Rules. Let's Start in These Four Areas*, WASH. POST (March 30, 2019), https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-821a-11e9-a3f7-78b7525a8d5f_story.html?utm_term=.6247ef86cd32.
2. See *Id.*
3. Facebook Privacy Principles, Facebook, <https://www.facebook.com/about/basics/privacy-principles> (last visited Aug. 16, 2019).
4. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC, 2016 O.J. L 119/1, art. 20 [hereinafter GDPR].
5. CAL. CIV. CODE § 1798.100(d) (effective Jan. 1, 2020).
6. Zuckerberg, *supra* note 1.
7. See *About Us*, DATA TRANSFER PROJECT, <https://datatransferproject.dev/> (last visited Aug. 16, 2019).
8. See Jacques Crémer, et al., *Competition Policy for the Digital Era*, Report for the European Commission (2019), <http://ec.europa.eu/competition/publications/reports/kd0419045enn.pdf>.
9. See Jason Furman et al., *Unlocking Digital Competition*, Report of the Digital Competition Expert Panel 9 (2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf ("There may be situations where opening up some of the data held by digital businesses and providing access on reasonable terms is the essential and justified step needed to unlock competition. Any remedy of this kind would need to protect personal privacy and consider carefully whether the benefits justified the impact on the business holding the data").
10. See, e.g., Datum Future, *Data Portability: What is at stake?* (July 2019), <https://www.datumfuture.org/wp-content/uploads/2019/07/Datum-Future-Data-Portability-July-2019.pdf>.
11. See Article 29 Data Protection Working Party, *Guidelines on the Right to Data Portability*, at 19 (2017), http://ec.europa.eu/newsroom/document.cfm?doc_id=44099 [hereinafter Art. 29 Working Party, Guidelines].
12. *Id.* at 11.
13. See, e.g., INFORMATION COMMISSIONER'S OFFICE, MONETARY PENALTY NOTICE (Oct. 24, 2018), <https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf>; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, PIPEDA REPORT OF FINDINGS #2019-002 (Apr. 26, 2019), <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/>; Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief, *United States v. Facebook, Inc.*, No. 19-cv-2184 (F.T.C. July 24, 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf [hereinafter Facebook Decision and Order].
14. See Art. 29 Working Party, *Guidelines*, *supra* note 11, at 19.
15. See *Id.* at 6 (emphasis added).
16. Furman et al., *supra* note 9, at 80.
17. These challenges go beyond the traditional data security challenges that arise in making personal data accessible through technical means (although those challenges are, in and of themselves, quite substantial). The risk of inadvertent disclosure or data leakage inevitably grows as the ways to access systems increase. The complex, independent systems that are needed to implement data portability will necessarily create additional ways to access data and controlled services—which may translate to greater security risks to users. See generally JOHN PALFREY & URS GASSER, *BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES* (2011).
18. See Art. 29 Working Party, *Guidelines*, *supra* note 11, at 5.
19. INTERNATIONAL ORGANIZATION FOR STANDARDISATION, ISO/IEC 19941:2017, *Information Technology – Cloud Computing – Interoperability and Portability* (2017), <https://www.iso.org/obp/ui/#iso:std:66639:en>.
20. See Facebook Decision and Order, *supra* note 13. But see Separate Statement of Commissioner Noah Joshua Phillips, *Federal Trade Commission v. Unrollme Inc.*, No. 1723139 (Aug. 8, 2019), https://www.ftc.gov/system/files/documents/public_statements/1539865/phillips_-_unrollme_statement_8-8-19.pdf (suggesting that Google's restriction of third parties from using the information in the Gmail accounts of consumers for purposes such as market research or advertising, while promoted as a means to enhance consumer privacy, may also limit consumer choice and competition).
21. See sources cited *supra* note 13.
22. Facebook Decision and Order, *supra* note 13.

END NOTES

23. See, e.g., Ben Thompson, *The Bill Gates Line Follow-up, Twitter and the Bill Gates Line, Data Portability and Facebook*, STRATEGY (May 29, 2016), <https://strategy.com/2016/the-bill-gates-line-follow-up-twitter-and-the-bill-gates-line-data-portability-and-facebook/> (acknowledging that “forced data portability and interoperability” would “return[] Facebook to the state it was with the original social graph API,” which is what prompted Cambridge Analytica); Ben Thompson, *The Facebook Brand*, STRATEGY (Mar. 19, 2016), <https://strategy.com/2016/the-facebook-brand/> (noting that Facebook Graph API allowed users to “give away everything about their friends” and “this is exactly how the researcher implicated in the Cambridge Analytica story” gained access to Facebook user data); Paul Przemysław Polański, *Some Thoughts on Data Portability in the Aftermath of the Cambridge Analytica Scandal*, 7 J. OF EUR. CONSUMER AND MARKET L. 141 (2018) (describing Cambridge Analytica as the result of flawed API implementation and calling for a conservative construction of the data portability right).
24. There are various technical means for accomplishing these transfers, and researchers are currently developing multi-lateral models that allow individuals to manage their data and decide where to store it. For example, personal information management systems (“PIMS”) let individuals store their data either locally or via cloud-based storage and let them “define at a sufficiently granular level how their personal information should be used and for what purposes.” See Eur. Data Protection Supervisor, EDPS Opinion on Personal Information Management Systems, Opinion 9/2016, at 7 (Oct. 20, 2016), https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf. In addition, an MIT project, “Solid,” aims to create “decentralized social applications” that will allow individuals to move their information wherever they choose and switch between multiple platforms. See CSAIIL-MIL, *What Does Solid Offer?*, Solid, <https://solid.mit.edu/> (last visited May 22, 2019). The Data Mobility Infrastructure Sandbox began evaluating the viability of data portability facilitated by entities like PIMS earlier this year. See CTRL-SHIFT, *Data Mobility Infrastructure Sandbox* (2019), https://www.ctrl-shift.co.uk/wp-content/uploads/2019/06/DMIS_June_2019_Downloadable_Singles_Final4.pdf.
25. Third parties who receive Covered Information through “a User-initiated transfer of Covered Information as part of a data portability protocol or standard” are not necessarily subject to the same controls and safeguards as third parties who receive Covered Information through other means. See Facebook Decision and Order, *supra* note 13.
26. GDPR, art. 20(1).
27. See Art. 29 Working Party, *Guidelines*, *supra* note 11, at 9.
28. The importance of ensuring that new requirements do not overburden smaller companies is a theme that has been sounded by many U.S. policymakers crafting privacy legislation. Several privacy bills contain certain exceptions for small entities. The DASHBOARD Act put forth by Sens. Mark Warner (D-VA) and Josh Hawley (R-MO), for example, limits its applicability to entities that “(1) generate a material amount of revenue from the use, collection, processing, sale, or sharing of the user data; and (2) have more than 100,000,000 unique monthly users in the United States for a majority of months during the previous 1-year period.” See Press Release, Sen. Mark R. Warner, Warner & Hawley Introduce Bill to Force Social Media Companies to Disclose How They Are Monetizing User Data (June 24, 2019), <https://www.warner.senate.gov/public/index.cfm/2019/6/warner-hawley-introduce-bill-to-force-social-media-companies-to-disclose-how-they-are-monetizing-user-data>. As another example, in a recent hearing Rep. Jan Schakowsky (D-IL) noted that “[w]e must not lose sight of small and medium-sized businesses and how heavy-handed laws and regulations can hurt them. Established bigger companies can navigate a complex and burdensome privacy regime. But millions of dollars in compliance costs aren’t doable for startups and small businesses.” See *Protecting Consumer Privacy in the Era of Big Data, Hearing Before the Subcomm. on Consumer Prot. of the Comm. on Energy & Commerce*, 116th Cong. (2019) (statement of Rep. Jan Schakowsky, Subcomm. Chair). Similarly, EU policymakers have sought to avoid disproportionate burdens on small- and medium-sized enterprises by legislating exceptions to certain data protection obligations. See, e.g., GDPR, art. 30(5) (exempting SMEs with 250 or fewer employees from certain GDPR record-keeping obligations). The GDPR also seeks to minimize disproportionate burdens on providers by permitting controllers to refuse to comply with data subject rights where requests are “manifestly unfounded or excessive, in particular because of their repetitive character.” See GDPR, art. 12(5)(b).
29. See, e.g., Dr. Aysem Diker Vanberg, *The Right to Data Portability in the GDPR: What Lessons Can Be Learned from the EU Experience*, 21(7) J. INTERNET L., 1, 3 (2018) (“[A]llowing one user to transfer a second user’s information to another platform may violate the privacy rights of a second user.”); Helena Ursic, *Unfolding the New-Born Right to Data Portability: Four Gateways to Data Subject Control*, 15(1) SCRIPT-ED 42, 56 (2018), <https://script-ed.org/wp-content/uploads/2018/08/ursic.pdf> (noting “additional difficulties in applying the right to data portability” when data contains “multiple persons’ data which are . . . intertwined”); Barbara Engels, *Data Portability Among Online Platforms*, 5 INTERNET POL’Y REV., June 2016, 4–5, <https://policyreview.info/articles/analysis/data-portability-among-online-platforms> (“Allowing one to transfer a second user’s information may violate the privacy rights of second user.”).
30. See Comments of New America’s Open Technology Institute, *In re Competition and Consumer Protection in The 21st Century: The Intersection Between Privacy, Big Data, and Competition*, at 4 (FTC, Aug. 20, 2018), https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-a-0034-154926.pdf [hereinafter OTI Comments] (“[N]owhere is [the tension between the right to portability and friends’ right of privacy] greater than when it comes to the portability of information about your contacts on social networks, or your ‘social graph.’”).
31. See, e.g., Ira Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, 3 INT’L DATA PRIVACY L. 74, 74–87 (2013), (supporting the idea of a property-based model of personal data that protects privacy); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056 (2003), <https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1066&context=facpubs> (developing a model of propertized personal information that protects privacy); see also Peter Swire & Yionni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare, Antitrust and Privacy Critique*, 72 MO. L. REV. 335, 373 (2013) (suggesting that right to data portability

END NOTES

- "appears more closely akin to the personal data ownership theory" than the right of access, and acknowledging debate around whether personal information is property).
32. See, e.g., Hayley Tsukayama, *Knowing the "Value" of Our Data Won't Fix Our Privacy Problems*, ELECTRONIC FRONTIER FOUNDATION (July 15, 2019), <https://www.eff.org/deeplinks/2019/07/knowning-value-our-data-won't-fix-our-privacy-problems>; Sarah Jeong, *Selling Your Private Information Is a Terrible Idea*, N.Y. TIMES (July 8, 2019), <https://www.nytimes.com/2019/07/08/opinion/health-data-property-privacy.html>.
33. See Eur. Commission, Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy (Jan. 10, 2017), <https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy>; see also Cameron F. Kerry & John B. Morris, *Why Data Ownership Is the Wrong Approach to Protecting Privacy*, BROOKINGS INSTITUTION (June 26, 2019), <https://www.brookings.edu/blog/techtank/2019/06/26/why-data-ownership-is-the-wrong-approach-to-protecting-privacy/>.
34. Similar considerations could apply when determining how to address privacy issues in connection with business-to-business transfers of data (which, as noted above, are beyond the scope of this paper, but just as important to enabling competition as the individual right to data portability). In the context of these transfers, there are often additional factors present that can greatly impact the privacy issues around the transfer.
35. See Bennett Cyphers & Danny O'Brien, *Facing Facebook: Data Portability and Interoperability Are Anti-Monopoly Medicine*, ELECTRONIC FRONTIER FOUNDATION (July 24, 2018), <https://www.eff.org/deeplinks/2018/07/facing-facebook-data-portability-and-interoperability-are-anti-monopoly-medicine>; Kevin Bankston, *How We Can "Free" Our Facebook Friends*, NEW AMERICA WEEKLY (June 28, 2018), <https://www.newamerica.org/weekly/edition-211/how-we-can-free-our-facebook-friends>; see also Orla Lynskey, *Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability*, EUR. L. REV. 793, 804-05 (2017) ("[T]he inability to access ['friends' data] could constitute a barrier to entry for potential competitors."). But see Thompson, *The Bill Gates Line Follow-up*, *supra* note 23.
36. See, e.g., OTI Comments, *supra* note 30, at 4 ("Most services will now let you download your own social media posts, but what about other people's comments to those posts, or your comments and tags on other people's posts and photos? These are just some of the examples of the unresolved tension between my right to portability and my friends' right to privacy, and nowhere is that tension greater than when it comes to the portability of information about your contacts on social networks, or your 'social graph'"); Lynskey, *supra* note 35, at 808 ("A further potential cost and complication for data controllers will be ensuring data security, given the tension between data security and data access. The A29WP perhaps underestimates the extent of this challenge for data controllers stating simply that the GDPR right may also 'raise some security issues' while highlighting that the data controller will remain responsible for 'taking all the security measures needed to ensure that personal data is securely transmitted[.]'"); Vonberg, *supra* note 29, at 7 ("The Article 29 Working Party arguably has not succeeded in offering more clarity as to what security standards are expected.").
37. See Art. 29 Working Party, *Guidelines*, *supra* note 11, at 19.
38. See PERSONAL DATA PROTECTION COMMISSION OF SINGAPORE, DISCUSSION PAPER ON DATA PORTABILITY 20 (Feb. 28, 2019), <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/Data-Portability/PDPC-CCCS-Data-Portability-Discussion-Paper---280219.pdf> [hereinafter PDPC Discussion Paper].
39. See PERSONAL DATA PROTECTION COMMISSION OF SINGAPORE, PUBLIC CONSULTATION ON REVIEW OF THE PERSONAL DATA PROTECTION ACT OF 2012 – PROPOSED DATA PORTABILITY AND DATA INNOVATION PROVISIONS 17 (May 22, 2019) [hereinafter PDPC Public Consultation].
40. See Gennie Gebhart, *Bennet Cyphers & Kurt Opsahl, What We Mean When We Say "Data Portability"*, ELECTRONIC FRONTIER FOUNDATION (Sept. 13, 2018), <https://www.eff.org/deeplinks/2018/09/what-we-mean-when-we-say-data-portability>; Bankston, *supra* note 35.
41. Notification fatigue is a problem often discussed in the breach notification context. See, e.g., Jeri Clausung, *'Security Fatigue' Complicates the Battle Against Data Breaches*, INTERNET SOC'Y (Dec. 21, 2016), <https://www.internetsociety.org/blog/2016/12/security-fatigue-complicates-the-battle-against-data-breaches/>; Christopher Mele, *Data Breaches Keep Happening. So Why Don't You Do Something?*, N.Y. TIMES (Aug. 1, 2018), <https://www.nytimes.com/2018/08/01/technology/data-breaches.html>.
42. See Bankston, *supra* note 35; Josh Constine, *Facebook Shouldn't Block You from Finding Friends on Competitors*, TECHCRUNCH (Apr. 13, 2018), <https://techcrunch.com/2018/04/13/free-the-social-graph/>; Cyphers & O'Brien, *supra* note 35; see also Lynskey, *supra* note 35, at 804-05 ("[T]he inability to access ['friends' data] could constitute a barrier to entry for potential competitors."). But see Thompson, *The Bill Gates Line Follow-up*, *supra* note 23.
43. See OTI Comments, *supra* note 30, at 6-7.
44. *Id.* at 7.
45. See, e.g., sources cited *supra* note 13.
46. Art. 29 Working Party, *Guidelines*, *supra* note 11, at 19.
47. *Id.*
48. See PDPC Discussion Paper, *supra* note 38, at 20; Gus Rossi & Charlotte Slatman, *Interoperability = Privacy + Competition*, PUBLIC KNOWLEDGE (Apr. 26, 2019), <https://www.publicknowledge.org/news-blog/blogs/interoperability-privacy-competition> ("[B]ecause they are dealing with personal data, third parties that want to interoperate would be required to follow a clear and transparent open model for user privacy, including potential requirements for pre-approval or certification by an independent entity").
49. See, e.g., GDPR, art. 42-43.
50. The Personal Data Protection Commission of Singapore recently proposed that it be given the power to issue binding codes of practice for sectors related to consumer safeguards, counterparty assurance, interoperability, and security of data. See PDPC Public Consultation, *supra* note 39, at 17 (the codes of practice would provide minimum standards for interoperability and security, criteria to verify the identity of recipient organizations prior to transfer, and information that must be provided to consumers to enable them to exercise their right to data portability).
51. See Art. 29 Working Party, *Guidelines*, *supra* note 11, at 6-7.
52. See Discussion Paper, *supra* note 38, at 20.
53. See PDPC Public Consultation, *supra* note 39, at 14.
54. Art. 29 Working Party, *Guidelines*, *supra* note 11, at 11.

EXHIBIT 4

הי אמיר - להלן סיכום של החיפוש - בבקשה תקרא (אני יודע שזה FW: 15:00 משעמם) ובוא נדבר ב-15:00

email: "ehudb@meitar.com Ehud Ben Ari"

Wednesday, March 20, 2019 at 7:40:31 PM Israel Standard Time

To: email: "alon@brandtotal.com 'Alon Leibovich'"

FYI

Ehud Ben Ari, Senior Associate

Meitar Liquornik Geva Leshem Tal, Law Offices

16 Abba Hillel Rd. Ramat Gan 5250608,
ISRAEL

Tel - 972-3-6863041

www.meitar.com

לוגו אנגלית עבה
להדפסות פרסום.jpg

This email message and any attachments thereto are confidential and/or privileged and/or subject to privacy laws and are intended only for use by the addressee(s) named above. If you are not the intended addressee, you are hereby kindly notified that any dissemination, distribution, copying or use of this email and any attachments thereto is strictly prohibited. If you have received this email in error, kindly delete it from your computer

system and notify us at the telephone number or email address appearing above. The writer asserts in respect of this message and attachments all rights for confidentiality, privilege or privacy to the fullest extent permitted by law.

Thank you.

From: Ehud Ben Ari

Sent: Wednesday, March 20, 2019 7:31 PM

To: Amir Leshman <amir@brandtotal.com>

Subject: 15:00- בוא נדבר ב-15:00 (אני יודע שזה משעמם) בבקשה תקרא - להלן סיכום של החיפוש -

Alon and Amir,

Following our call, below is a short summary and analysis of what Brandtotal ("BT") is collecting and whether it is permitted under the current terms of service of Facebook (<https://www.facebook.com/terms.php>: "Facebook Terms").

The main prohibition under the Facebook Terms – Clause 3, section 3, sub-section 3:

"You may not access or collect data from our Products using automated means (without our prior permission) or attempt to access data you do not have permission to access"

An analysis of this sentence leads to two use cases where data gathering is not permitted.

The first, accessing data or collecting data from
"Products" using automated means.

What are the "Products"? they are defined as (<https://www.facebook.com/help/1561485474074139?ref=tos>): "

...Facebook (including the Facebook mobile app and in-app browser), Messenger, Instagram (including apps like Direct and Boomerang), Portal-branded devices, Moments, Bonfire, Facebook Mentions, Spark AR Studio, Audience Network, and any other features, apps, technologies, software, products, or services offered by Facebook Inc. or Facebook Ireland Limited under our Data Policy. The Facebook Products also include Facebook Business Tools, which are tools used by website owners and publishers, app developers, business partners (including advertisers) and their customers to support business services and exchange information with Facebook, such as social plugins (like the "Like" or "Share" button) and our SDKs and APIs"

This means that any data collected, using automated means, from what is defined products, cannot be collected.

The second use case is attempting to access data **(a user) does not have permission to access**. This would probably include an direct contact with a Facebook "private" API that is not open to such end user.

What kind of data is BT using/collecting?

1.

Data the end user is exposed to.

Per our call, generally speaking, when an end user uses a BT extension or app, the end user provides BT with two kinds of data: (i) data that is provided by the end user via the extension/app where T is passive all kinds of data ("Passive End User Collection") and (ii) data which is collected when BT **actively** uses the extension to connect with Facebook via API and/or "calls" to gather data ("Active End User Collection").

(A)

Collection of Ads the End User is exposed to:

Passive End User Collection of the Ads the end user is exposed to. This collection of the Ads the end user is exposed to

should be permitted under the Facebook Terms as (i) this data is not part of the Facebook Products definition (and so it does not conflict with the abovementioned prohibition) and (ii) it doesn't fall under a data the end user is not permitted to access as this is the very data that Facebook strives to provide to the end user.

Active End User Collection of the Ads the end user is exposed to. This collection is in a grey area. Why? Because here the collection is not provided by the End User, but is performed by BT. And so, on the one hand, one can claim that given this data is not part of the "Products" definition then access to such data should be fine as it is not owned by Facebook. On the other hand, actively activating the API in order to see the Ads, where BT is not an End User, prohibits the covenant not to collect data which one does not have permission to access.

(B)

End User Demographic and End User Posts.

While the End User provides Facebook with a license to use such content and demographics, it still belongs to the End User (Clause 3, section 3, sub-section 1 – *"Permission to use content you create and share: You own the content you create and share on Facebook and the other Facebook Products you use, and nothing in these Terms takes away the rights you have to your own content"*). And so, if the End User provides BT with such data (i.e. Passive Data Collection) that should be permitted under the Facebook Terms.

2.

Posts about a business Facebook page:

If BT's client created the business Facebook page, and the client wishes for BT to collect information related to

such Facebook business page, then collection of such data using automated collection of data is

prohibited under the Facebook Terms (https://www.facebook.com/policies/pages_groups_events/):

"Your Page, Group or Event must not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without written permission from Facebook."

A possible solution, though not perfect and not without risk a claim by Facebook against BT is to only collect data which is publicly accessible. If that data is accessible from a simple search via a search engine, then one can claim that Facebook cannot prohibit collection of such data.

3.

Data gathered from a direct link by BT to a Facebook API (and not via an End User)

It would appear, from the Facebook Terms for Developers (<https://developers.facebook.com/policy/>) Clause 3, section 9, that such

collection is prohibited as BT may not sell the data it receives from Facebook's services.

Ehud Ben Ari, Senior Associate

Meitar Liquornik Geva Leshem Tal, Law Offices

16 Abba Hillel Rd. Ramat Gan 5250608,
ISRAEL

Tel - 972-3-6863041

www.meitar.com

לוגו אנגלית עבה
להדפסות פרסום.jpg

This email message and any attachments thereto are confidential and/or privileged and/or subject to privacy laws and are intended only for use by the addressee(s) named above. If you are not the intended addressee, you are hereby kindly notified that any dissemination, distribution, copying or use of this email and any attachments thereto is strictly prohibited. If you have received this email in error, kindly delete it from your computer system and notify us at the telephone number or email address appearing above. The writer asserts in respect of this message and attachments all rights for confidentiality, privilege or privacy to the fullest extent permitted by law.

Thank you.

EXHIBIT 5

EXHIBIT FILED UNDER
SEAL

EXHIBIT 6



Terms of Service

Terms of Service

[Paid Service Terms of Service](#)

[Paid Service Usage Rules](#)

[Collecting Society Notices](#)

[Copyright Notices](#)

[Community Guidelines](#)

What's in these terms?

This index is designed to help you understand some of the key updates we've made to our Terms of Service (Terms). We hope this serves as a useful guide, but please ensure you read the Terms in full.

Welcome to YouTube!

This section outlines our relationship with you. It includes a description of the Service, defines our Agreement, and names your service provider.

Who May Use the Service?

This section sets out certain requirements for use of the Service, and defines categories of users.

Your Use of the Service

This section explains your rights to use the Service, and the conditions that apply to your use of the Service. It also explains how we may make changes to the Service.

Your Content and Conduct

This section applies to users who provide Content to the Service. It defines the scope of the permissions that you grant by uploading your Content, and includes your agreement not to upload anything that infringes on anyone else's rights.

Account Suspension and Termination

This section explains how you and YouTube may terminate this relationship.

About Software in the Service

This section includes details about software on the Service.

Other Legal Terms

This section includes our service commitment to you. It also explains that there are some things we will not be responsible for.

About this Agreement

This section includes some further important details about our contract, including what to expect if we need to make changes to these Terms; or which law applies to them.

Terms of Service

Dated: January 5, 2022

TERMS OF SERVICE

Welcome to YouTube!

Introduction

Thank you for using the YouTube platform and the products, services and features we make available to you as part of the platform (collectively, the “Service”).

Our Service

The Service allows you to discover, watch and share videos and other content, provides a forum for people to connect, inform, and inspire others across the globe, and acts as a distribution platform for original content creators and advertisers large and small. We provide lots of information about our products and how to use them in our [Help Center](#).

Among other things, you can find out about [YouTube Kids](#), the [YouTube Partner Program](#) and [YouTube Paid Memberships and Purchases](#) (where available). You can also read all about enjoying content on [other devices like your television, your games console, or Google Home](#).

Your Service Provider

The entity providing the Service is Google LLC, a company operating under the laws of Delaware, located at 1600 Amphitheatre Parkway, Mountain View, CA 94043 (referred to as “**YouTube**”, “**we**”, “**us**”, or “**our**”). References to YouTube’s “**Affiliates**” in these terms means the other companies within the Alphabet Inc. corporate group (now or in the future).

Applicable Terms

Your use of the Service is subject to these terms, the [YouTube Community Guidelines](#) and the [Policy, Safety and Copyright Policies](#) which may be updated from time to time (together, this “**Agreement**”). Your Agreement with us will also include the [Advertising on YouTube Policies](#) if you provide advertising or sponsorships to the Service or incorporate paid promotions in your content. Any other links or references provided in these terms are for informational use only and are not part of the Agreement.

Please read this Agreement carefully and make sure you understand it. If you do not understand the Agreement, or do not accept any part of it, then you may not use the Service.

Who may use the Service?

Age Requirements

You must be at least 13 years old to use the Service; however, children of all ages may use the Service and YouTube Kids (where available) if enabled by a parent or legal guardian.

Permission by Parent or Guardian

If you are under 18, you represent that you have your parent or guardian's permission to use the Service. Please have them read this Agreement with you.

If you are a parent or legal guardian of a user under the age of 18, by allowing your child to use the Service, you are subject to the terms of this Agreement and responsible for your child's activity on the Service. You can find tools and resources to help you manage your family's experience on YouTube (including how to enable a child under the age of 13 to use the Service and YouTube Kids) in our [Help Center](#) and through Google's [Family Link](#).

Businesses

If you are using the Service on behalf of a company or organisation, you represent that you have authority to act on behalf of that entity, and that such entity accepts this Agreement.

Your Use of the Service

Content on the Service

The content on the Service includes videos, audio (for example music and other sounds), graphics, photos, text (such as comments and scripts), branding (including trade names, trademarks, service marks, or logos), interactive features, software, metrics, and other materials whether provided by you, YouTube or a third-party (collectively, "Content").

Content is the responsibility of the person or entity that provides it to the Service. YouTube is under no obligation to host or serve Content. If you see any Content you believe does not comply with this Agreement, including by violating the [Community Guidelines](#) or the law, you can [report it to us](#).

Google Accounts and YouTube Channels

You can use parts of the Service, such as browsing and searching for Content, without having a [Google account](#). However, you do need a Google account to use some

features. With a Google account, you may be able to like videos, subscribe to channels, create your own YouTube channel, and more. You can follow these instructions to [create a Google account](#).

Creating a YouTube channel will give you access to additional features and functions, such as uploading videos, making comments or creating playlists (where available). Here are some details about how to [create your own YouTube channel](#).

To protect your Google account, keep your password confidential. You should not reuse your Google account password on third-party applications. Learn more about [keeping your Google account secure](#), including what to do if you learn of any unauthorized use of your password or Google account.

Your Information

Our [Privacy Policy](#) explains how we treat your personal data and protect your privacy when you use the Service. The [YouTube Kids Privacy Notice](#) provides additional information about our privacy practices that are specific to YouTube Kids.

We will process any audio or audiovisual content uploaded by you to the Service in accordance with the [YouTube Data Processing Terms](#), except in cases where you uploaded such content for personal purposes or household activities. [Learn More](#).

Permissions and Restrictions

You may access and use the Service as made available to you, as long as you comply with this Agreement and applicable law. You may view or listen to Content for your personal, non-commercial use. You may also show YouTube videos through the embeddable YouTube player.

The following restrictions apply to your use of the Service. You are not allowed to:

1. access, reproduce, download, distribute, transmit, broadcast, display, sell, license, alter, modify or otherwise use any part of the Service or any Content except: (a) as expressly authorized by the Service; or (b) with prior written permission from YouTube and, if applicable, the respective rights holders;
2. circumvent, disable, fraudulently engage with, or otherwise interfere with any part of the Service (or attempt to do any of these things), including security-related features or features that (a) prevent or restrict the copying or other use of Content or (b) limit the use of the Service or Content;
3. access the Service using any automated means (such as robots, botnets or scrapers) except (a) in the case of public search engines, in accordance with YouTube's robots.txt file; or (b) with YouTube's prior written permission;
4. collect or harvest any information that might identify a person (for example, usernames or faces), unless permitted by that person or allowed under section (3) above;
5. use the Service to distribute unsolicited promotional or commercial content or other unwanted or mass solicitations;
6. cause or encourage any inaccurate measurements of genuine user engagement with the Service, including by paying people or providing them with incentives to increase a video's views, likes, or dislikes, or to increase a channel's subscribers, or otherwise manipulate metrics in any manner;
7. misuse any reporting, flagging, complaint, dispute, or appeals process, including by making groundless, vexatious, or frivolous submissions;
8. run contests on or through the Service that do not comply with [YouTube's contest policies and guidelines](#);

9. use the Service to view or listen to Content other than for personal, non-commercial use (for example, you may not publicly screen videos or stream music from the Service); or

10. use the Service to (a) sell any advertising, sponsorships, or promotions placed on, around, or within the Service or Content, other than those allowed in the [Advertising on YouTube](#) policies (such as compliant product placements); or (b) sell advertising, sponsorships, or promotions on any page of any website or application that only contains Content from the Service or where Content from the Service is the primary basis for such sales (for example, selling ads on a webpage where YouTube videos are the main draw for users visiting the webpage).

Reservation

Using the Service does not give you ownership of or rights to any aspect of the Service, including user names or any other Content posted by others or YouTube.

Develop, Improve and Update the Service

YouTube is constantly changing and improving the Service. As part of this continual evolution, we may make modifications or changes (to all or part of the Service) such as adding or removing features and functionalities, offering new digital content or services or discontinuing old ones. We may also need to alter or discontinue the Service, or any part of it, in order to make performance or security improvements, make changes to comply with law, or prevent illegal activities on or abuse of our systems. These changes may affect all users, some users or even an individual user. When the Service requires or includes downloadable software (such as the YouTube Studio application), that software may update automatically on your device once a new version or feature is available, subject to your device settings. If we make material changes that negatively impact your use of the Service, we'll provide you with reasonable advance notice, except in urgent

situations such as preventing abuse, responding to legal requirements, or addressing security and operability issues. We'll also provide you with an opportunity to export your content from your Google Account using [Google Takeout](#), subject to applicable law and policies.

Your Content and Conduct

Uploading Content

If you have a YouTube channel, you may be able to upload Content to the Service. You may use your Content to promote your business or artistic enterprise. If you choose to upload Content, you must not submit to the Service any Content that does not comply with this Agreement (including the [YouTube Community Guidelines](#)) or the law. For example, the Content you submit must not include third-party intellectual property (such as copyrighted material) unless you have permission from that party or are otherwise legally entitled to do so. You are legally responsible for the Content you submit to the Service. We may use automated systems that analyze your Content to help detect infringement and abuse, such as spam, malware, and illegal content.

Rights you Grant

You retain ownership rights in your Content. However, we do require you to grant certain rights to YouTube and other users of the Service, as described below.

License to YouTube

By providing Content to the Service, you grant to YouTube a worldwide, non-exclusive, royalty-free, sublicensable and transferable license to use that Content (including to reproduce, distribute, prepare derivative works, display and perform it) in connection with the Service and YouTube's (and its successors' and Affiliates') business, including for the purpose of promoting and redistributing part or all of the Service.

License to Other Users

You also grant each other user of the Service a worldwide, non-exclusive, royalty-free license to access your Content through the Service, and to use that Content, including to reproduce, distribute, prepare derivative works, display, and perform it, only as enabled by a feature of the Service (such as video playback or embeds). For clarity, this license does not grant any rights or permissions for a user to make use of your Content independent of the Service.

Duration of License

The licenses granted by you continue for a commercially reasonable period of time after you remove or delete your Content from the Service. You understand and agree, however, that YouTube may retain, but not display, distribute, or perform, server copies of your videos that have been removed or deleted.

Right to Monetize

You grant to YouTube the right to monetize your Content on the Service (and such monetization may include displaying ads on or within Content or charging users a fee for access). This Agreement does not entitle you to any payments. Starting November 18, 2020, any payments you may be entitled to receive from YouTube under any other agreement between you and YouTube (including for example payments under the YouTube Partner Program, Channel memberships or Super Chat) will be treated as royalties. If required by law, Google will withhold taxes from such payments.

Removing Your Content

You may [remove your Content](#) from the Service at any time. You also have the option to [make a copy of your Content](#) before removing it. You must remove your Content if you no longer have the rights required by these terms.

Removal of Content By YouTube

If any of your Content (1) is in breach of this Agreement or (2) may cause harm to YouTube, our users, or third parties, we reserve the right to remove or take down some or all of such Content in our discretion. We will notify you with the reason for our action unless we reasonably believe that to do so: (a) would breach the law or the direction of a legal enforcement authority or would otherwise risk legal liability for YouTube or our Affiliates; (b) would compromise an investigation or the integrity or operation of the Service; or (c) would cause harm to any user, other third party, YouTube or our Affiliates. You can learn more about reporting and enforcement, including how to appeal on the [Troubleshooting](#) page of our Help Center.

Community Guidelines Strikes

YouTube operates a system of “strikes” in respect of Content that violates the [YouTube Community Guidelines](#). Each strike comes with varying restrictions and may result in the permanent removal of your channel from YouTube. A full description of how a strike affects your channel is available on the [Community Guidelines Strikes Basics](#) page. If you believe that a strike has been issued in error, you may appeal [here](#).

If your channel has been restricted due to a strike, you must not use another channel to circumvent these restrictions. Violation of this prohibition is a material breach of this Agreement and Google reserves the right to terminate your Google account or your access to all or part of the Service.

Copyright Protection

We provide information to help copyright holders manage their intellectual property online in our [YouTube Copyright Center](#). If you believe your copyright has been infringed on the Service, please [send us a notice](#).

We respond to notices of alleged copyright infringement according to the process in our [YouTube Copyright Center](#), where you can also find information about how to resolve a copyright strike. YouTube's policies provide for the termination, in appropriate circumstances, of repeat infringers' access to the Service.

Account Suspension & Termination

Terminations by You

You may stop using the Service at any time. Follow these [instructions](#) to delete the Service from your Google Account, which involves closing your YouTube channel and removing your data. You also have the option to download a copy of your data first.

Terminations and Suspensions by YouTube

YouTube reserves the right to suspend or terminate your Google account or your access to all or part of the Service if (a) you materially or repeatedly breach this Agreement; (b) we are required to do so to comply with a legal requirement or a court order; or (c) we reasonably believe that there has been conduct that creates (or could create) liability or harm to any user, other third party, YouTube or our Affiliates.

Notice for Termination or Suspension

We will notify you with the reason for termination or suspension by YouTube unless we reasonably believe that to do so: (a) would violate the law or the direction of a legal enforcement authority; (b) would compromise an investigation; (c) would compromise the integrity, operation or security of the Service; or (d) would cause harm to any user, other third party, YouTube or our Affiliates.

Effect of Account Suspension or Termination

If your Google account is terminated or your access to the Service is restricted, you may continue using certain aspects

of the Service (such as viewing only) without an account, and this Agreement will continue to apply to such use. If you believe that the termination or suspension has been made in error, you can [appeal using this form](#).

About Software in the Service

Downloadable Software

When the Service requires or includes downloadable software (such as the YouTube Studio application), unless that software is governed by additional terms which provide a license, YouTube gives you a personal, worldwide, royalty-free, non-assignable and non-exclusive license to use the software provided to you by YouTube as part of the Service. This license is for the sole purpose of enabling you to use and enjoy the benefit of the Service as provided by YouTube, in the manner permitted by this Agreement. You are not allowed to copy, modify, distribute, sell, or lease any part of the software, or to reverse-engineer or attempt to extract the source code of that software, unless laws prohibit these restrictions or you have YouTube's written permission.

Open Source

Some software used in our Service may be offered under an open source license that we make available to you. There may be provisions in an open source license that expressly override some of these terms, so please be sure to read those licenses.

Other Legal Terms

Warranty Disclaimer

OTHER THAN AS EXPRESSLY STATED IN THIS AGREEMENT OR AS REQUIRED BY LAW, THE SERVICE IS PROVIDED "AS IS" AND YOUTUBE DOES NOT MAKE ANY SPECIFIC COMMITMENTS OR WARRANTIES ABOUT THE SERVICE. FOR EXAMPLE, WE DON'T MAKE ANY WARRANTIES ABOUT: (A) THE CONTENT PROVIDED THROUGH THE SERVICE; (B) THE SPECIFIC FEATURES OF THE SERVICE, OR ITS ACCURACY, RELIABILITY, AVAILABILITY, OR ABILITY TO MEET YOUR

NEEDS; OR (C) THAT ANY CONTENT YOU SUBMIT WILL BE ACCESSIBLE ON THE SERVICE.

Limitation of Liability

EXCEPT AS REQUIRED BY APPLICABLE LAW, YOUTUBE, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES AND AGENTS WILL NOT BE RESPONSIBLE FOR ANY LOSS OF PROFITS, REVENUES, BUSINESS OPPORTUNITIES, GOODWILL, OR ANTICIPATED SAVINGS; LOSS OR CORRUPTION OF DATA; INDIRECT OR CONSEQUENTIAL LOSS; PUNITIVE DAMAGES CAUSED BY:

1. ERRORS, MISTAKES, OR INACCURACIES ON THE SERVICE;
2. PERSONAL INJURY OR PROPERTY DAMAGE RESULTING FROM YOUR USE OF THE SERVICE;
3. ANY UNAUTHORIZED ACCESS TO OR USE OF THE SERVICE;
4. ANY INTERRUPTION OR CESSATION OF THE SERVICE;
5. ANY VIRUSES OR MALICIOUS CODE TRANSMITTED TO OR THROUGH THE SERVICE BY ANY THIRD PARTY;
6. ANY CONTENT WHETHER SUBMITTED BY A USER OR YOUTUBE, INCLUDING YOUR USE OF CONTENT; AND/OR
7. THE REMOVAL OR UNAVAILABILITY OF ANY CONTENT.

THIS PROVISION APPLIES TO ANY CLAIM, REGARDLESS OF WHETHER THE CLAIM ASSERTED IS BASED ON WARRANTY, CONTRACT, TORT, OR ANY OTHER LEGAL THEORY.

YOUTUBE AND ITS AFFILIATES' TOTAL LIABILITY FOR ANY CLAIMS ARISING FROM OR RELATING TO THE SERVICE IS LIMITED TO THE GREATER OF: (A) THE AMOUNT OF REVENUE THAT YOUTUBE HAS PAID TO YOU FROM YOUR USE OF THE SERVICE IN THE 12 MONTHS BEFORE THE DATE OF YOUR NOTICE, IN WRITING TO YOUTUBE, OF THE CLAIM; AND (B) USD \$500.

Indemnity

To the extent permitted by applicable law, you agree to defend, indemnify and hold harmless YouTube, its Affiliates, officers, directors, employees and agents, from and against any and all claims, damages, obligations, losses, liabilities, costs or debt, and expenses (including but not limited to attorney's fees) arising from: (i) your use of and access to the Service; (ii) your violation of any term of this Agreement; (iii) your violation of any third party right, including without limitation any copyright, property, or privacy right; or (iv) any claim that your Content caused damage to a third party. This defense and indemnification obligation will survive this Agreement and your use of the Service.

Third-Party Links

The Service may contain links to third-party websites and online services that are not owned or controlled by YouTube. YouTube has no control over, and assumes no responsibility for, such websites and online services. Be aware when you leave the Service; we suggest you read the terms and privacy policy of each third-party website and online service that you visit.

About this Agreement

Changing this Agreement

We may change this Agreement, for example, (1) to reflect changes to our Service or how we do business - for example, when we add new products or features or remove old ones, (2) for legal, regulatory, or security reasons, or (3) to prevent abuse or harm.

If we materially change this Agreement, we'll provide you with reasonable advance notice and the opportunity to review the changes, except (1) when we launch a new product or feature, or (2) in urgent situations, such as preventing ongoing abuse or responding to legal requirements. If you don't agree to the new terms, you should remove any Content you uploaded and stop using the Service.

Continuation of this Agreement

If your use of the Service ends, the following terms of this Agreement will continue to apply to you: “Other Legal Terms”, “About This Agreement”, and the licenses granted by you will continue as described under “Duration of License”.

Severance

If it turns out that a particular term of this Agreement is not enforceable for any reason, this will not affect any other terms.

No Waiver

If you fail to comply with this Agreement and we do not take immediate action, this does not mean that we are giving up any rights that we may have (such as the right to take action in the future).

Interpretation

In these terms, “include” or “including” means “including but not limited to,” and any examples we give are for illustrative purposes.

Governing Law

All claims arising out of or relating to these terms or the Service will be governed by California law, except California’s conflict of laws rules, and will be litigated exclusively in the federal or state courts of Santa Clara County, California, USA. You and YouTube consent to personal jurisdiction in those courts.

Limitation on Legal Action

YOU AND YOUTUBE AGREE THAT ANY CAUSE OF ACTION ARISING OUT OF OR RELATED TO THE SERVICES MUST COMMENCE WITHIN ONE (1) YEAR AFTER THE CAUSE OF ACTION ACCRUES. OTHERWISE, SUCH CAUSE OF ACTION IS PERMANENTLY BARRED.

Effective as of January 5, 2022 ([view previous version](#))

EXHIBIT 7

Hello
Select your address

All ▾

Hello, Sign in
Account & Lists ▾Returns
& Orders
[All](#)
[Best Sellers](#)
[Amazon Basics](#)
[New Releases](#)
[Customer Service](#)
[Today's Deals](#)
[Amazon Outlet](#)
[Support small, shop women-owned](#)

Help & Customer Service

[◀ All Help Topics](#)

Legal Policies

[3rd Party Licensing Notice \(Mobile App\)](#)

Conditions of Use

[Amazon.com Privacy Notice](#)
[Amazon Group Companies](#)
[Amazon Trademark Usage Guidelines](#)
[Non-Exhaustive List of Amazon Trademarks](#)
[Amazon.com Gift Card and Electronic Message Customization Service Terms](#)

Quick solutions


Your Orders
Track or cancel orders

Returns & Refunds
Exchange or return items

Manage Prime
Cancel or view benefits

Payment Settings
Add or edit payment methods

Carrier Info
Shipping carrier information

Account Settings
Change email or password

Find more solutions


[Security and Privacy](#) › [Legal Policies](#) ›

Conditions of Use

Last updated: May 3, 2021

Welcome to Amazon.com. Amazon.com Services LLC and/or its affiliates ("Amazon") provide website features and other products and services to you when you visit or shop at Amazon.com, use Amazon products or services, use Amazon applications for mobile, or use software provided by Amazon in connection with any of the foregoing (collectively, "Amazon Services"). By using the Amazon Services, you agree, on behalf of yourself and all members of your household and others who use any Service under your account, to the following conditions.

Please read these conditions carefully.

We offer a wide range of Amazon Services, and sometimes additional terms may apply. When you use an Amazon Service (for example, Your Profile, Gift Cards, Amazon Video, Your Media Library, Amazon devices, or Amazon applications) you also will be subject to the guidelines, terms and agreements applicable to that Amazon Service ("Service Terms"). If these Conditions of Use are inconsistent with the Service Terms, those Service Terms will control.

PRIVACY

Please review our [Privacy Notice](#), which also governs your use of Amazon Services, to understand our practices.

ELECTRONIC COMMUNICATIONS

When you use Amazon Services, or send e-mails, text messages, and other communications from your desktop or mobile device to us, you may be communicating with us electronically. You consent to receive communications from us electronically, such as e-mails, texts, mobile push notices, or notices and messages on this site or through the other Amazon Services, such as our Message Center, and you can retain copies of these communications for your records. You agree that all agreements, notices, disclosures, and other communications that we provide to you electronically satisfy any legal requirement that such communications be in writing.

COPYRIGHT

All content included in or made available through any Amazon Service, such as text, graphics, logos, button icons, images, audio clips, digital downloads, data compilations, and software is the property of Amazon or its content suppliers and protected by United States and international copyright laws. The compilation of all content included in or made available through any Amazon Service is the exclusive property of Amazon and protected by U.S. and international copyright laws.

TRADEMARKS

[Click here to see a non-exhaustive list of Amazon trademarks.](#) In addition, graphics, logos, page headers, button icons, scripts, and service names included in or made available through any Amazon Service are trademarks or trade dress of Amazon in the U.S. and other countries. Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon that appear in any Amazon Service are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

PATENTS

One or more patents owned by Amazon apply to the Amazon Services and to the features and services accessible via the Amazon Services. Portions of the Amazon Services operate under license of one or more patents. [Click here to see a non-exhaustive list of applicable Amazon patents and applicable licensed patents.](#)

LICENSE AND ACCESS

Subject to your compliance with these Conditions of Use and any Service Terms, and your payment of any applicable fees, Amazon or its content providers grant you a limited, non-exclusive, non-transferable, non-sublicensable license to access and make personal and non-commercial use of the Amazon Services. This license does not include any resale or commercial use of any Amazon Service, or its contents; any collection and use of any product listings, descriptions, or prices; any derivative use of any Amazon Service or its contents; any downloading, copying, or other use of account information for the benefit of any third party; or any use of data mining, robots, or similar data gathering and extraction tools. All rights not expressly granted to you in these Conditions of Use or any Service Terms are reserved and retained by Amazon or its licensors, suppliers, publishers, rightsholders, or other content providers. No Amazon Service, nor any part of any Amazon Service, may be reproduced, duplicated, copied, sold, resold, visited, or otherwise exploited for any commercial purpose without express written consent of Amazon. You may not frame or utilize framing techniques to enclose any trademark, logo, or other proprietary information (including images, text, page layout, or form) of Amazon without express written consent. You may not use any meta tags or any other "hidden text" utilizing Amazon's name or trademarks without the express written consent of Amazon. You may not misuse the Amazon Services. You may use the Amazon Services only as permitted by law. The licenses granted by Amazon terminate if you do not comply with these Conditions of Use or any Service Terms.

YOUR ACCOUNT

You may need your own Amazon account to use certain Amazon Services, and you may be required to be logged in to the account and have a valid payment method associated with it. If there is a problem charging your selected payment method, we may charge any other valid payment method associated with your account. Visit [Your Payments](#) to manage your payment options. You are responsible for maintaining the confidentiality of your account and password and for restricting access to your account, and you agree to accept responsibility for all activities that occur under your account or password. Amazon does sell products for children, but it sells them to adults, who can purchase with a credit card or other permitted payment method. If you are under 18, you may use the Amazon Services only with involvement of a parent or guardian. Parents and guardians may create profiles for teenagers in their Amazon Household. Alcohol listings on Amazon are intended for adults. You must be at least 21 years of age to purchase alcohol, or use any site functionality related to alcohol. Amazon reserves the right to refuse service, terminate accounts, terminate your rights to use Amazon Services, remove or edit content, or cancel orders in its sole discretion.

REVIEWS, COMMENTS, COMMUNICATIONS, AND OTHER CONTENT

You may post reviews, comments, photos, videos, and other content; send e-cards and other communications; and submit suggestions, ideas, comments, questions, or other information, so long as the content is not illegal, obscene, threatening, defamatory, invasive of privacy, infringing of intellectual property rights (including publicity rights), or otherwise injurious to third parties or objectionable, and does not consist of or contain software viruses, political campaigning, commercial solicitation, chain letters, mass mailings, or any form of "spam" or unsolicited commercial electronic messages. You may not use a false e-mail address, impersonate any person or entity, or otherwise mislead as to the origin of a card or other content. Amazon reserves the right (but not the obligation) to remove or edit such content, but does not regularly review posted content.

If you do post content or submit material, and unless we indicate otherwise, you grant Amazon a nonexclusive, royalty-free, perpetual, irrevocable, and fully sublicensable right to use, reproduce, modify, adapt, publish, perform, translate, create derivative works from, distribute, and display such content throughout the world in any media. You grant Amazon and sublicensees the right to use the name that you submit in connection with such content, if they choose. You represent and warrant that you own or otherwise control all of the rights to the content that you post; that the content is accurate; that use of the content you supply does not violate this policy and will not cause injury to any person or entity; and that you will indemnify Amazon for all claims resulting from content you supply. Amazon has the right but not the obligation to monitor and edit or

remove any activity or content. Amazon takes no responsibility and assumes no liability for any content posted by you or any third party.

INTELLECTUAL PROPERTY COMPLAINTS

Amazon respects the intellectual property of others. If you believe that your intellectual property rights are being infringed, please follow our [Notice and Procedure for Making Claims of Copyright Infringement](#)

RISK OF LOSS

All purchases of physical items from Amazon are made pursuant to a shipment contract. This means that the risk of loss and title for such items pass to you upon our delivery to the carrier.

RETURNS, REFUNDS AND TITLE

Amazon does not take title to returned items until the item arrives at our fulfillment center. At our discretion, a refund may be issued without requiring a return. In this situation, Amazon does not take title to the refunded item. For more information about our returns and refunds, please see our [Returns Center](#).

PRODUCT DESCRIPTIONS

Amazon attempts to be as accurate as possible. However, Amazon does not warrant that product descriptions or other content of any Amazon Service is accurate, complete, reliable, current, or error-free. If a product offered by Amazon itself is not as described, your sole remedy is to return it in unused condition.

PRICING

"List Price" means the suggested retail price of a product as provided by a manufacturer, supplier, or seller. We regularly check List Prices against prices recently found on Amazon and other retailers. Certain products may have a "Was Price" displayed, which is determined using recent price history of the product on Amazon.

With respect to items sold by Amazon, we cannot confirm the price of an item until you order. Despite our best efforts, a small number of the items in our catalog may be mispriced. If the correct price of an item sold by Amazon is higher than our stated price, we will, at our discretion, either contact you for instructions before shipping or cancel your order and notify you of such cancellation. Other merchants may follow different policies in the event of a mispriced item.

We generally do not charge your credit card until after your order has entered the shipping process or, for digital products, until we make the digital product available to you.

APP PERMISSIONS

When you use apps created by Amazon, such as the Amazon App or Kindle App, you may grant certain permissions to us for your device. Most mobile devices provide you with information about these permissions. To learn more about these permissions, [click here](#).

SANCTIONS AND EXPORT POLICY

You may not use any Amazon Service if you are the subject of U.S. sanctions or of sanctions consistent with U.S. law imposed by the governments of the country where you are using Amazon Services. You must comply with all U.S. or other export and re-export restrictions that may apply to goods, software (including Amazon Software), technology, and services.

OTHER BUSINESSES

Parties other than Amazon operate stores, provide services or software, or sell product lines through the Amazon Services. In addition, we provide links to the sites of affiliated companies and certain other businesses. If you purchase any of the products or services offered by these businesses or individuals, you are purchasing directly from those third parties, not from Amazon. We are not responsible for examining or evaluating, and we do not warrant, the offerings of any of these businesses or individuals (including the content of their Web sites). Amazon does not assume any responsibility or liability for the actions, product, and content of all these and any other third parties. You should carefully review their privacy statements and other conditions of use.

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITY

THE AMAZON SERVICES AND ALL INFORMATION, CONTENT, MATERIALS, PRODUCTS (INCLUDING SOFTWARE) AND OTHER SERVICES INCLUDED ON OR OTHERWISE MADE

AVAILABLE TO YOU THROUGH THE AMAZON SERVICES ARE PROVIDED BY AMAZON ON AN "AS IS" AND "AS AVAILABLE" BASIS, UNLESS OTHERWISE SPECIFIED IN WRITING. AMAZON MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, AS TO THE OPERATION OF THE AMAZON SERVICES, OR THE INFORMATION, CONTENT, MATERIALS, PRODUCTS (INCLUDING SOFTWARE) OR OTHER SERVICES INCLUDED ON OR OTHERWISE MADE AVAILABLE TO YOU THROUGH THE AMAZON SERVICES, UNLESS OTHERWISE SPECIFIED IN WRITING. YOU EXPRESSLY AGREE THAT YOUR USE OF THE AMAZON SERVICES IS AT YOUR SOLE RISK.

TO THE FULL EXTENT PERMISSIBLE BY LAW, AMAZON DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. AMAZON DOES NOT WARRANT THAT THE AMAZON SERVICES, INFORMATION, CONTENT, MATERIALS, PRODUCTS (INCLUDING SOFTWARE) OR OTHER SERVICES INCLUDED ON OR OTHERWISE MADE AVAILABLE TO YOU THROUGH THE AMAZON SERVICES, AMAZON'S SERVERS OR ELECTRONIC COMMUNICATIONS SENT FROM AMAZON ARE FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS. TO THE FULL EXTENT PERMISSIBLE BY LAW, AMAZON WILL NOT BE LIABLE FOR ANY DAMAGES OF ANY KIND ARISING FROM THE USE OF ANY AMAZON SERVICE, OR FROM ANY INFORMATION, CONTENT, MATERIALS, PRODUCTS (INCLUDING SOFTWARE) OR OTHER SERVICES INCLUDED ON OR OTHERWISE MADE AVAILABLE TO YOU THROUGH ANY AMAZON SERVICE, INCLUDING, BUT NOT LIMITED TO DIRECT, INDIRECT, INCIDENTAL, PUNITIVE, AND CONSEQUENTIAL DAMAGES, UNLESS OTHERWISE SPECIFIED IN WRITING.

DISPUTES

Any dispute or claim relating in any way to your use of any Amazon Service will be adjudicated in the state or Federal courts in King County, Washington, and you consent to exclusive jurisdiction and venue in these courts. We each waive any right to a jury trial.

APPLICABLE LAW

By using any Amazon Service, you agree that applicable federal law, and the laws of the state of Washington, without regard to principles of conflict of laws, will govern these Conditions of Use and any dispute of any sort that might arise between you and Amazon.

SITE POLICIES, MODIFICATION, AND SEVERABILITY

Please review our other policies, such as our [pricing policy](#), posted on this site. These policies also govern your use of Amazon Services. We reserve the right to make changes to our site, policies, Service Terms, and these Conditions of Use at any time. If any of these conditions shall be deemed invalid, void, or for any reason unenforceable, that condition shall be deemed severable and shall not affect the validity and enforceability of any remaining condition.

OUR ADDRESS

Amazon.com, Inc.
P.O. Box 81226
Seattle, WA 98108-1226
<https://www.amazon.com>

ADDITIONAL AMAZON SOFTWARE TERMS

The following terms ("Software Terms") apply to any software (including any updates or upgrades to the software) and any related documentation we make available to you in connection with Amazon Services (the "Amazon Software").

1. **Use of the Amazon Software.** You may use Amazon Software solely for purposes of enabling you to use the Amazon Services as provided by Amazon, and as permitted by these Conditions of Use and any Service Terms. You may not incorporate any portion of the Amazon Software into other programs or compile any portion of it in combination with other programs, or otherwise copy (except to exercise rights granted in this section), modify, create derivative works of, distribute, assign any rights to, or license the Amazon Software in whole or in part. All software used in any Amazon Service is the property of Amazon or its software suppliers and is protected by United States and international copyright laws.
2. **Use of Third Party Services.** When you use the Amazon Software, you may also be using the services of one or more third parties, such as a wireless carrier or a mobile software

provider. Your use of these third party services may be subject to the separate policies, terms of use, and fees of these third parties.

3. **No Reverse Engineering.** You may not reverse engineer, decompile or disassemble, tamper with, or bypass any security associated with the Amazon Software, whether in whole or in part.
4. **Updates.** We may offer automatic or manual updates to the Amazon Software at any time and without notice to you.
5. **Government End Users.** If you are a U.S. Government end user, we are licensing the Amazon Software to you as a "Commercial Item" as that term is defined in the U.S. Code of Federal Regulations (see 48 C.F.R. § 2.101), and the rights we grant you to the Amazon Software are the same as the rights we grant to all others under these Conditions of Use.
6. **Conflicts.** In the event of any conflict between these Conditions of Use and any other Amazon or third-party terms applicable to any portion of Amazon Software, such as open-source license terms, such other terms will control as to that portion of the Amazon Software and to the extent of the conflict.

HOW TO SERVE A SUBPOENA OR OTHER LEGAL PROCESS

Amazon accepts service of subpoenas or other legal process only through Amazon's national registered agent, Corporation Service Company (CSC). Subpoenas or other legal process may be served by sending them to CSC at the following address:

Amazon.com, Inc.
Corporation Service Company
300 Deschutes Way SW, Suite 208 MC-CSC1
Tumwater, WA 98501
Attn: Legal Department - Legal Process

Please note also that providing detailed and accurate information at the outset will facilitate efficient processing of your request. That information will include, for example, e-mail and/or credit card number used to make purchases for retail purchase information; the name, e-mail, and physical address of a seller for seller information; device serial number for Amazon devices; and IP address and complete time stamps.

NOTICE AND PROCEDURE FOR MAKING CLAIMS OF INTELLECTUAL PROPERTY INFRINGEMENT

If you believe that your intellectual property rights have been infringed, please submit your complaint using our online [form](#). This form may be used to report all types of intellectual property claims including, but not limited to, copyright, trademark, and patent claims.

We respond quickly to the concerns of rights owners about any alleged infringement, and we terminate repeat infringers in appropriate circumstances.

We offer the following alternative to our online form for copyright complaints only. You may submit written claims of copyright infringement to our Copyright Agent at:

Copyright Agent
Amazon.com Legal Department
P.O. Box 81226
Seattle, WA 98108
phone: (206) 266-4064
e-mail: copyright@amazon.com

Courier address:
Copyright Agent
Amazon.com Legal Department
2021 7th Avenue
Seattle, WA 98121
USA

Written claims concerning copyright infringement must include the following information:

- A physical or electronic signature of the person authorized to act on behalf of the owner of the copyright interest;
- A description of the copyrighted work that you claim has been infringed upon;
- A description of where the material that you claim is infringing is located on the site;
- Your address, telephone number, and e-mail address;
- A statement by you that you have a good-faith belief that the disputed use is not authorized by the copyright owner, its agent, or the law; and
- A statement by you, made under penalty of perjury, that the above information in your notice is accurate and that you are the copyright owner or authorized to act on the copyright owner's behalf.

Was this information helpful?

Yes

No

[Back to top](#)

Get to Know Us

[Careers](#)
[Blog](#)
[About Amazon](#)
[Sustainability](#)
[Press Center](#)
[Investor Relations](#)
[Amazon Devices](#)
[Amazon Science](#)

Make Money with Us

[Sell products on Amazon](#)
[Sell apps on Amazon](#)
[Become an Affiliate](#)
[Become a Delivery Driver](#)
[Start a package delivery business](#)
[Advertise Your Products](#)
[Self-Publish with Us](#)
[Host an Amazon Hub](#)
[› See More Ways to Make Money](#)

Amazon Payment Products

[Amazon Rewards Visa Signature Cards](#)
[Amazon Store Card](#)
[Amazon Secured Card](#)
[Amazon Business Card](#)
[Amazon Business Line of Credit](#)
[Shop with Points](#)
[Credit Card Marketplace](#)
[Reload Your Balance](#)
[Amazon Currency Converter](#)

Let Us Help You

[Amazon and COVID-19](#)
[Your Account](#)
[Your Orders](#)
[Shipping Rates & Policies](#)
[Amazon Prime](#)
[Returns & Replacements](#)
[Manage Your Content and Devices](#)
[Amazon Assistant](#)
[Help](#)



English

United States

Amazon Music
Stream millions of songs

Amazon Advertising
Find, attract, and engage customers

Amazon Drive
Cloud storage from Amazon

6pm
Score deals on fashion brands

AbeBooks
Books, art & collectibles

ACX
Audiobook Publishing Made Easy

Alexa
Actionable Analytics for the Web

Sell on Amazon
Start a Selling Account

Amazon Business
Everything For Your Business

Amazon Fresh
Groceries & More Right To Your Door

AmazonGlobal
Ship Orders Internationally

Home Services
Experienced Pros Happiness Guarantee

Amazon Ignite
Sell your original Digital Educational Resources

Amazon Web Services
Scalable Cloud Computing Services

Audible
Listen to Books & Original Audio Performances

Book Depository
Books With Free Delivery Worldwide

Box Office Mojo
Find Movie Box Office Data

ComiXology
Thousands of Digital Comics

DPRReview
Digital Photography

Fabric
Sewing, Quilting & Knitting

Goodreads
Book reviews & recommendations

IMDb
Movies, TV & Celebrities

IMDbPro

Kindle Direct

Amazon Photos

Prime Video

Shopbop
Designer Fashion Brands

Amazon Warehouse
Great Deals on Quality Used Products

Get Info
Entertainment
Professionals
Need

Whole Foods Market
America's Healthiest
Grocery Store

Publishing
Indie
Digital &
Print
Publishing
Made Easy

Woot!
Deals and
Shenanigans

Unlimited Photo
Storage
Free With Prime

Zappos
Shoes &
Clothing

Direct
Video
Distribution
Made Easy

Ring
Smart Home
Security
Systems

eero WiFi
Stream 4K
Video
in Every
Room

Amazon
Subscription
Boxes
Top
subscription
boxes – right
to your door

Blink
Smart Security
for Every Home

PillPack
Pharmacy
Simplified

Neighbors App
Real-Time Crime
& Safety Alerts

Amazon
Renewed
Like-new
products
you can
trust

Conditions of Use

Privacy Notice

Interest-Based Ads

© 1996-2022, Amazon.com, Inc. or its affiliates

EXHIBIT 8



LinkedIn Service Terms

December 13, 2021

The following Service Terms apply to Customer to the extent the specific Service is included in the applicable ordering document. LinkedIn may update these Service Terms from time to time. LinkedIn reserves the right to upgrade, update or discontinue any aspect or feature of a Service in whole or in part; provided, however, that if LinkedIn discontinues a Service in whole during the term of an ordering document, then LinkedIn will provide Customer with an alternative or replacement service.

1. TALENT SERVICES

1.1. Recruiter Corporate

Customer will use the Recruiter Corporate Service (and related services) and information about Members only to recruit individuals to become employees and consultants of Customer or its Affiliates, or, if Customer is acting as a Staffing Agency or BPO, only to recruit individuals to become employees and consultants of its clients. "Staffing Agency" means a Customer that uses the Services to recruit on behalf of a third-party client using Customer's own name and/or logo, including without limitation, staffing agencies, executive search firms, and direct hire firms. "BPO" means a business process outsourcer Customer that recruits on behalf of a client using the client's name and/or logo, including without limitation, recruitment process outsourcers, managed service providers, and clinical research outsourcers. Customer will inform LinkedIn of its Staffing Agency or BPO classification with a client before purchasing the Recruiter Corporate Service, and Agency will promptly inform LinkedIn of any change in classification. Staffing Agency purchases of Recruiter Corporate seats are governed by the master subscription agreement between LinkedIn and Staffing Agency. BPO purchases of Recruiter Corporate seats are governed by



Agreement.

1.2. Recruiter Professional

Customer will use the Recruiter Professional Service and related services ("RPS") and information about Members only to recruit individuals to become employees and consultants of its clients. Only Staffing Agencies may use RPS. Customer is prohibited from using RPS to recruit on behalf of a client using the client's name and/or logo. Customer will inform LinkedIn of its Staffing Agency classification with a client before purchasing RPS, and Staffing Agency will promptly inform LinkedIn of any change in classification. Customer's breach of this Section will be deemed a material breach of the Agreement.

1.3. Recruiter Lite

Customer will use the Recruiter Lite Service (and related services) and information about Members only to recruit individuals to become employees and consultants of Customer or its Affiliates, or, if Customer is a Staffing Agency, only to recruit individuals to become employees and consultants of its clients. BPOs are prohibited from using the Recruiter Lite Service. Excluding BPOs, Customer's and its Affiliates' employees and contractors are limited to a cumulative total of 20 Recruiter Lite seats. Customer's breach of this Section will be deemed a material breach of the Agreement.

1.4. Additional Terms for Recruiter

Recruiter seats may be reassigned in accordance with the terms set forth on the [Recruiter Help Portal](#). Customer will not share any information regarding a LinkedIn Member's Open to Opportunities status with that Member's current employer. Customer will ensure that its Customer Users use the Recruiter InMail feature in accordance with LinkedIn's [Recruiter InMail Policy](#). Customer's breach of this Section will be deemed a material breach of the Agreement.



The Job Postings and Job Slots Services (collectively, the Jobs Services) are designed to help Customer reach quality candidates for job opportunities. Job Postings posted under available Job Slots will expire upon the expiration/termination of the ordering document. The Jobs Services allow Customer's postings to be served on properties (e.g., websites and mobile applications) of LinkedIn and enabled third parties. Customer is responsible for (i) all postings and content through the Jobs Services or otherwise to LinkedIn, including but not limited to the job descriptions, creatives, trademarks, images, URLs and pixels that comprise the postings or content therefor (collectively, the "Postings"); and (ii) all content and property to which Postings may direct viewers, as well as redirects ("Destinations"). Customer may not resell or transfer access to the Jobs Services to any other party. Each Posting must be for 1 job opportunity; it is not permitted for a Posting to solicit applications for more than one position. Customer will not copy, duplicate, replicate, scrape or otherwise reproduce jobs from a hiring company's website and upload them to LinkedIn as Postings without the hiring company's prior knowledge and authorization. Where a hiring company informs LinkedIn that Customer has done so without its prior knowledge and authorization, LinkedIn reserves the right to remove such Postings immediately and without prior notice to Customer. In order to post a job for a position at a third-party entity, Customer must have an active contract in place with the third-party entity providing active recruiting services beyond job posting for the applicable position. Customer agrees that it will not, and will not enable or authorize any third party, by virtue of the Postings, Destinations, or use of the Jobs Services, to:

- Create Postings without a reasonable and legitimate intent to hire for a bona fide job opportunity or the specific position listed;
- Create Postings that intentionally misrepresent the job, hiring company, or poster;
- Fail to clearly disclose in any Posting that a position is for an independent contractor or is part-time, piecework, commission-based,



-
- Create Postings for “business opportunities” that require payments or recruitment of others or that resemble franchises, multi-level marketing, club memberships, distributorships, or are entirely or almost entirely commission-based;
 - Provide identifiable candidate resume or application data to any other parties;
 - “Spam” or otherwise contact applicants for purposes other than related to the specific employment opportunity described in the posting;
 - Harass, stalk, or contact any applicant after they have asked not to be contacted;
 - Create Postings in the United States without possessing valid Federal or State Employer Identification Numbers, if applicable, or create Postings in any other location in a manner that would not allow compliance with applicable tax and employment laws;
 - Create Postings for jobs that require applicants to pay for employment or otherwise bear costs related to employment in violation of applicable law;
 - Soliciting employees by intentional misrepresentation;
 - Create Postings, advertise employment positions, or otherwise engage in recruitment or hiring practices that would be a violation of the law in Customer’s state or country, the state or country where the job is to be performed, or the applicable laws of the jurisdiction that governs the LSA between the parties;
 - Engage in solicitations, communications or transactions that violate any applicable laws or regulations related to the prohibition of employment
-



- Engage in illegal or fraudulent conduct;
- Except as expressly authorized by LinkedIn in writing, use any automated means or form of scraping or data extraction to access, modify, download, query or otherwise collect information from LinkedIn's websites;
- Except as expressly authorized by LinkedIn in writing, copy, modify or create derivative works of the Jobs Services or any related technology; or
- Create Postings that contain malware, spyware or any other malicious code or otherwise interfere with the operation of the Jobs Services or any device or system or breach or circumvent any security measure of LinkedIn or a third party.

1.6. Career Pages

All Career page "traffic driver" ad impressions will launch within 90 days from the Start Date in the ordering document, using social ad units and targeting generated by LinkedIn.

1.7. Talent Hub

Talent Hub is a hiring platform that enables customers to source, manage, and hire candidates in one place. Talent Hub is a system of record that is an applicant management system designed to host all candidate data, including first name and last name, email address, telephone number, professional history, interview and hiring team feedback and evaluations, salary information, final disposition, and other candidate data received from Customer's third-party talent acquisition extensions ("Talent Hub Data"). Talent Hub will be used to manage candidates through the recruiting workflow ultimately helping companies collaborate on jobs and candidates and hire in the same platform



in the aggregate to surface insights and benchmarking to help companies have better insight into their process relative to their peers. Customer is solely responsible for the implementation of Talent Hub, including (i) migrating any candidate data from Customer's third-party applicant tracking system to Talent Hub; (ii) providing the candidate data in a format that is acceptable to LinkedIn and compatible with Talent Hub; and (iii) ensuring it has all necessary consents to provide the candidate data to LinkedIn (collectively, the "Implementation"). LinkedIn disclaims any and all liability in connection with the Implementation.

2. SALES SERVICES

2.1. Sales Navigator

Customer may use the Sales Navigator Service only to generate sales leads. Customer may not use the Sales Navigator Service for recruiting purposes. Customer will have access to Sales Navigator **value-add services** for the Term of the ordering document. No refund or credit will be provided if the value-add services are not used during the Term of the ordering document.

3. LEARNING SERVICES

3.1. lynda.com for Library (LyndaLibrary)

Customer will have access to the content on the **lynda.com** platform only. A Customer User must be a library patron. For lynda.com Customers only, the User Agreement does not apply. Customer will designate a single administrator and that administrator will have access to the reporting and management tools. Users of the content on the lynda.com platform are subject to the **Lynda.com Privacy Policy**. For each LyndaLibrary seat purchased by Customer, any Customer User who has a valid Customer's library card, pin/password may access the learning content via lynda.com for Library during the term of the order. A Customer User is an individual designated by Customer



Customer's geographical service location. Customer must verify that the individual resides in the Customer's geographical service location. A Customer User may be a staff member even if the staff member does not reside in Customer's geographical service location. Customer may only market the LyndaLibrary service to individual patrons of the Library. Customer or any government entity related to or associated with Customer will not market to any other groups, including but not limited to, any business, corporation, school district, school (including higher education such as universities or colleges), non-profits, and government agencies. Customer's breach of the foregoing sentence will be considered a material breach of the Agreement. If LinkedIn determines that Customer or any other entity is marketing the LyndaLibrary without permission, LinkedIn will terminate Customer's order. Customer will not be able to establish sub administrators, upload content, reassign seats, or display or perform the content in a public setting, including a conference room or classroom. The concurrent number of Customer Users who can access the Lynda content at any one time is limited to the number of seats purchased by Customer.

3.2. LinkedIn Learning

Customer will have access to the content on the LinkedIn.com platform only. Customer Users may only view the content online via the LinkedIn.com platform or by downloading the content for offline viewing via the LinkedIn Learning mobile app. Customer may not violate the intellectual property or other rights of LinkedIn, including, without limitation, (i) copying or distributing our learning videos or other materials or (ii) using the word "LinkedIn" or our logos in any business name, email, or URL except as provided in the **Brand Guidelines**. Unless agreed to otherwise by the parties on the applicable ordering document, a Customer User must be a then current employee, contractor, student or library patron depending upon the LinkedIn Learning service purchased by Customer. For the LinkedIn Learning service, the User Agreement will apply if Customer connects its LinkedIn Learning dashboard to its Customer Users' LinkedIn.com profiles. Customer



reporting and management tools and will be able to establish full administrators and sub administrators with limited rights and access. Except as set forth below, Customer may only display or perform the content in a public setting, including a conference room or classroom, if Customer has purchased seats for all Customer Users. Customer retains sole responsibility for all content (including third-party content) uploaded or provided by Customer through our Services and will monitor, review, and remove such content. All content Customer uploads or provides through our Services must be owned or licensed to Customer. Only Customer will have access to such content. One LinkedIn Learning seat = One Customer User, and each seat is deemed used/active when a Customer User registers to access the content service. Each Customer User must have a unique identifier for a login, such as a unique email address or IP address. Aliases are not permitted. During each 12-month term of an ordering document, Customer may reassign 10 seats or 25% of the total number of seats purchased, whichever is greater. For LinkedIn Learning Campus, the number of seat reassignments is equal to 10 seats or 35% of the total number of seats purchased, whichever is greater. During the term of a LinkedIn Campus ordering document, should the Campus Customer exceed the total FTE count listed on the ordering document Customer may increase the FTE count with an executed, zero-dollar add-on ordering document. The add-on seats will co-term with the original order form. If the original ordering document is for a Partial Campus (a specific department on Campus) the additional zero-dollar seats requested must be used for said specific department only. LinkedIn Campus FTE quantities listed on the initial invoice represent the starting quantities that will be provisioned by LinkedIn.

3.2.1. LinkedIn Learning for Library

For each LinkedIn Learning for Library seat purchased by Customer, any Customer User who has a valid Customer's library card, or pin/password, may access the LinkedIn Learning content via LinkedIn Learning for Library during the term of the order. The LinkedIn User Agreement will not apply to LinkedIn Learning for Library Customer Users. A Customer User is an individual



valid address) in Customer's geographical service location. Customer must verify that the individual resides in the Customer's geographical service location. A Customer User may be a staff member even if the staff member does not reside in Customer's geographical service location. Customer may only market the LinkedIn Learning for Library service to individual patrons of the Library. Customer or any government entity related to or associated with Customer will not market to any other groups, including but not limited to, any business, corporation, school district, school (including higher education such as universities or colleges), non-profits, and government agencies. Customer's breach of the foregoing sentence will be considered a material breach of the Agreement. If LinkedIn determines that Customer or any other entity is marketing LinkedIn Learning for Library without permission, LinkedIn will terminate Customer's order. Customer will not be able to establish sub administrators, upload content, reassign seats, or display or perform the content in a public setting, including a conference room or classroom.

4. INSIGHTS SERVICES

4.1. Custom Insights & Analytics Reports

LinkedIn may generate certain insights and analytics reports on Customer's behalf derived from aggregating applicable Member profile data ("Insights Reports"). LinkedIn, in its sole discretion, may adjust or decline to include certain Member profile data in Insights Reports if LinkedIn believes the exposure of the Member profile data may compromise the privacy of Members or other LinkedIn customers. Insights Reports generated by LinkedIn on Customer's behalf are considered delivered on the date the Insights Reports are sent to Customer, even if LinkedIn provides additional analysis of the Insights Reports at a later date (e.g. responses to follow-up questions, modifications, etc.). LinkedIn will not release any underlying LinkedIn data or third-party data used to generate Insights Reports. LinkedIn retains ownership of all right, title, and interest to all content included in the Insights Reports (including any associated intellectual property rights). LinkedIn hereby grants Customer a



Customer's non-commercial activity. Customer will be prohibited from externally publishing Insights Reports or sharing Insights Reports with third parties without LinkedIn prior written approval in each instance. Insights Services will expire upon the expiration of the ordering document, and Insights Reports are deemed delivered the earlier of the: (i) actual delivery or (ii) the expiration of the ordering document.

4.2. LinkedIn Talent Insights

The LinkedIn Talent Insights ("LTI") Service provide customers self-serve on-demand, real-time access to aggregated LinkedIn Member profile data. LinkedIn, in its sole discretion, may adjust or decline to include certain Member profile data in the LTI Service if LinkedIn believes the exposure of the Member profile data may compromise the privacy of Members or other LinkedIn customers. LinkedIn will not release any underlying LinkedIn data or third-party data used in the LTI Service. LinkedIn retains ownership of all right, title, and interest to all content included in the LTI Service (including any associated intellectual property rights). LTI Data is derived from LinkedIn member profiles and company pages and is provided "as-is". LinkedIn disclaims all liability regarding the quality, accuracy, completeness, and timeliness of the LTI Data. LinkedIn hereby grants Customer a non-exclusive, perpetual, royalty-free, worldwide, non-transferable, non-sublicensable license to use, distribute, and display reports and data generated via the LTI Service ("LTI Data") for Customer's internal use. Customer shall not (i) publish externally or share the LTI Data with third parties without LinkedIn's prior written approval in each instance; (ii) trade, sell/re-sell or otherwise monetize the LTI Service or LTI Data or access to the same, without LinkedIn's consent; (iii) scrape or aggregate the LTI Data for the purposes of creating a competing service; or (iv) use the LTI Service or LTI Data to inform pre-investment activities and/or public security investment activities for itself or its end-clients. Notwithstanding anything written in the LSA or any other agreement between the parties, (a) only Customer and the specific Customer Affiliates to which Customer has purchased LTI Services on behalf of under this Order Form



to accommodate personnel arising in connection with a Change of Control. “Change of Control” means (i) the sale of all or substantially all of Customer’s assets to a third-party; (ii) any change in the ownership of more than 50% of Customer’s voting capital stock in one or more related transactions; (iii) Customer’s purchase of all or substantially all of a third-party’s assets; (iv) Customer’s purchase of more than 50% of a third-party’s voting capital stock in one or more related transactions; and (v) any Customer merger, consolidation, or acquisition with, by, or into another entity. Pricing for add-on LTI Services requested in connection with a non-authorized Affiliate or a Change of Control will be at LinkedIn’s then-current list rates. Customer’s breach of this Section 4.2 will be considered a material breach of the Agreement.

4.3. LinkedIn Sales Insights.

The LinkedIn Sales Insights (“LSI”) Service provides customers self-serve on-demand, real-time access to aggregated LinkedIn company data. LinkedIn, in its sole discretion, may adjust or decline to include certain company data in the LSI Service if LinkedIn believes the exposure of the company data may compromise the privacy of Members or other LinkedIn customers. LinkedIn will not release any underlying LinkedIn data or third-party data used in the LSI Service. LinkedIn retains ownership of all right, title, and interest to all content included in the LSI Service (including any associated intellectual property rights). LinkedIn hereby grants Customer a non-exclusive, perpetual, royalty-free, worldwide, non-transferable, non-sublicensable license to use, distribute, and display reports and data generated via the LSI Service (“LSI Data”) for Customer’s *internal use only*. Customer **shall not** (i) publish externally or share the LSI Data with third parties without LinkedIn’s prior written approval in each instance; (ii) trade, sell/re-sell or otherwise monetize the LSI Service or LSI Data or access to the same, without LinkedIn’s written consent; (iii) scrape or aggregate the LSI Data for the purposes of creating a competing service; (iv) use the LSI Data for securities investing and/or to inform merger & acquisition-based decisions; or (v) use the LSI Service or LSI Data for talent acquisition. LSI Data is derived from LinkedIn company pages, and **LinkedIn disclaims all**



document with LinkedIn specify a limit on the number of times LSI Data may be downloaded by Customer, such downloads must be completed during the contract term and may not be carried into a new contract period. If the term of Customer's Agreement or ordering document is greater than 12 months, the download limit is fixed annually and any unused downloads may not be carried into the subsequent year of the Agreement or ordering document. **Customer's breach of this Section 4.3 will be considered a material breach of the Agreement.** The LSI Service is non-cancelable and non-refundable.

5. TALENT MEDIA SERVICES

5.1. General

Customer authorizes LinkedIn to place advertisements ("Talent Media") containing artwork, copy, active URLs, and other advertising material and technology provided by Customer ("Advertising Materials") on LinkedIn websites and/or third-party network websites, subject to Customer electing to enable or disable the delivery of Talent Media on third-party network websites <https://www.linkedin.com/help/linkedin/answer/83628>) (collectively, the "Site"). Customer will submit to LinkedIn all Advertising Materials for Talent Media in accordance with LinkedIn's **Advertising Specifications and Guidelines** (collectively, "Ad Policies"). Customer will obtain all necessary rights, consents, licenses and clearances for LinkedIn to include the Advertising Materials in Talent Media. LinkedIn reserves the right, in its sole discretion, to reject or remove from the Site any Talent Media for which the Advertising Materials or the website to which the Talent media is linked (i) do not comply with the Ad Policies; (ii) do not comply with any applicable law, regulation, other judicial or administrative order, or industry self-regulatory principles; or (iii) may tend to bring, disparagement, ridicule, or scorn upon LinkedIn or its Affiliates. LinkedIn will use all Talent Media in compliance with this Agreement and any written instructions provided on the ordering document. LinkedIn's measurements are the definitive measurements for calculating fees. Third party impression tracking is unavailable for Talent



makes no guarantees as to (a) the results or distribution of any Talent Media in any manner; or (b) any number of sends, impressions, opens or clicks. No make goods or credit will be provided to Customer. LinkedIn does not screen or attempt to verify the accuracy of any information on the Site or in the Member profiles, and, as such, does not guarantee the identity or Personal Data of the individuals who will view the Talent Media purchased by Customer. Unless agreed to otherwise by the parties on the applicable ordering document: (i) Customer will pre-pay for Talent Media; (ii) Talent Media is non-cancellable and non-refundable; (iii) Talent Media will expire upon the expiration of the ordering document; and (iv) impressions are deemed delivered the earlier of (a) actual delivery or (b) the expiration of the ordering document. As provided in LinkedIn's [Privacy Policy](#), LinkedIn may use device identifiers obtained on and off the LinkedIn website for Talent Media, including to determine which devices Members may use and serve advertisements to them on their different devices. LinkedIn and Customer will each prominently post a complete and accurate privacy policy on their respective websites and mobile applications, including information regarding cross-device tracking and advertising targeting.

5.2. Recruitment Ads, Sponsored Jobs and Sponsored Updates

Recruitment Ads, Sponsored Jobs and Sponsored Updates are Talent Media sold under an auction model. The auction is a generalized second price auction and Customer only has to pay just enough to beat the second highest bidder. For example, if the winning advertiser has a bid of ten (\$10) dollars cost-per-click, but the next highest bid is seven (\$7) dollars, the winning advertiser only pays \$7.01. The second price method allows each advertiser to bid the absolute maximum they are willing to pay for the Talent Media. LinkedIn will charge enough to enable the highest price to be paid to win the auction.

5.3. Work With Us Ads



agreed in writing by LinkedIn. LinkedIn cannot identify all Members at a specific company because of company name inconsistencies. Inconsistencies arise because a Member can fill-out their “Company Name” field by either selecting a company name from a pre-existing list generated by the LinkedIn system or typing in their own custom company name. LinkedIn can only identify Members who have selected a company name from the pre-existing list.

5.4. Pipeline Builder

Customer will use the Pipeline Builder Service and information about Members only to recruit individuals to become employees and consultants of Customer or its Affiliates, or, if Customer is an approved agency, only to recruit individuals to become employees and consultants of its clients.

5.5. Talent Solutions Content Partner Program

If Customer is participating in the Talent Solutions Content Partner Program as set forth in the ordering document, then Customer will comply with the **Talent Solutions Content Partner Program Terms**.

6. ELEVATE SERVICE

Customer will maintain a social media policy and ensure that its personnel comply with the policy. Only Customer's designated curator(s) is/are authorized to post content to the Elevate Service. Customer Users, who are not curators, may only read and forward content. Customer will ensure that it owns or has the necessary licenses, rights, and consents to the content it posts to the Elevate Service.

7. GLINT SERVICES

7.1. Service Descriptions



manager that meets the minimum confidentiality threshold will receive a link to a dashboard and corresponding action plans that reflect the unique results of their team, (iii) role based permissions, data access and viewing privileges based on a user's role and organizational structure, (iv) Single Sign-On (SSO) using Supported Methods (Standard SAML 2.0 based integrations included) to allow one set of login credentials across multiple platforms, (v) comment analytics using Natural Language Processing (NLP) that is trained specifically on employee feedback and automatically extracts the most-discussed topics/themes, employee sentiment, and prescriptive/constructive comments in real-time, (vi) integrated action plans that are automatically generated for each manager based on the unique results of their team, including concrete steps and a pre-built library of resources from Glint, (vii) Glint's taxonomy, which has over 100 research driven questions across all the key domains of organizational development and the employee journey that can be drawn from to support each organization's unique needs, (viii) language translations for questions & communications in 50+ languages for standard questions and communication templates, (ix) smart alerts that automatically comb through all the survey results by various demographics and highlight key findings, such as outlier populations that have low scores, high scores, or significant changes in scores, and (x) communications templates for organization-wide and ad-hoc communications prior to, during, and post-survey. The Services do not include importing Customer data from third-party services, importing historical survey response data, exporting or transferring Customer data to any third-party services, or any integration of the Service with Customer or third-party software. Additional Fees will apply if Customer does not provide its data in a Glint-approved format. If no HRIS system is used, then additional Fees will apply if Glint does not receive the data in one compiled file. Customer Users may have access to a free, online community where they can, among other things, share best practices, which is not part of the Services.

7.1.2. If purchased, the Glint Engage Module includes Scheduled Recurring, Ad-Hoc & Always-On Surveys to measure employee engagement, team



relating to Survey responses in the dashboard, along with reporting that can be customized and saved for review. It also provides additional intelligence to understand the data, including but not limited to industry benchmarks, alerts and customizable data visualizations. Glint will provide access to the Service via a login for Authorized Users. Upon login, Customer will have access to the dashboard with Survey results by team and by driver with benchmark data, Survey management functionality (including question editing and frequency setting), and reporting (including Customer's ability to configure reports with various filters and date ranges and then to export reports).

7.1.3. If purchased, the Glint 360s Module is a multi-rater employee feedback tool intended to enable employees to obtain a holistic review of their strengths and growth opportunities based on input from peers, collaborators, direct reports and managers (such reviews, "360 Reviews"). This Module is intended to enable human resources professionals to quickly initiate 360 Reviews for Customer employees and to provide the employees with actionable feedback following the completion of the 360 Reviews. To activate and use the 360s Module, Customer must send HRIS data via regular exports from its HRIS System to the Glint Platform.

7.1.4. If purchased, the Glint Engage + Lifecycle Package includes all product features from the Glint Engage Module including Scheduled Recurring, Ad-Hoc & Always-On Surveys to measure employee engagement, team effectiveness, manager effectiveness, and/or diversity & inclusion, plus Glint's Employee Lifecycle program which extends feedback to key events in the employee journey such as onboarding, role changes, and exit through automatically triggered surveys.

7.1.5. If purchased, the Glint People Success Package provides access to all Glint product features to allow organizations to measure and deliver insight into the employee experience, launch development feedback programs, and provide suggested actions and learning. This bundle includes Glint's Engage, Lifecycle,



-
- **Pulse surveys** measure employee sentiment in real time, with programs spanning employee engagement, manager and team effectiveness, culture, diversity and inclusion and more
 - **Employee Lifecycle** captures feedback from critical moments in the employee journey such as onboarding, role changes, and exit through automatically triggered surveys
 - **Anytime Feedback** gives every employee the ability to seek, provide, and receive timely feedback, fostering greater self-awareness, continuous learning, and growth
 - **360 Feedback** gives managers the structured insights and guidance they need to develop as more effective leaders
 - **Integration with Microsoft Teams** nudge your people to provide feedback and view results in their flow of work
 - **Combined insights** across employee feedback programs and Workplace Analytics data give leaders a unique view into how people work impacts how they feel
 - **Interactive dashboards** and reports allow HR teams, leaders and managers to quickly make sense of the data, drill as deep as they want, and connect insight with outcomes like regrettable attrition and your organization's KPIs
 - **Smart Alerts** uses AI-for-HR™ to monitor millions of data points and generate real-time alerts for employee populations that are at-risk for increased
-

EXHIBIT 9

REDACTED VERSION
OF EXHIBIT FILED
UNDER SEAL

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

META PLATFORMS, INC., a
Delaware corporation,

Plaintiffs,

v.

BRANDTOTAL LTD., an Israeli
corporation, and UNIMANIA, INC.,
a Delaware corporation,

Defendants.

Civil Action No.: 3:20-CV-07182-JCS

Hon. Joseph C. Spero

OPENING EXPERT REPORT OF DAVID B. THAW, J.D., Ph.D.
JANUARY 12, 2022

I. Introduction

I, David Thaw, have been retained in this matter to offer an expert opinion (this “Opinion”) regarding certain questions pertaining to the cybersecurity risks associated with the software, applications, and other technologies developed and maintained by BrandTotal, Ltd. and its affiliates, including Unimania, Inc. (collectively, “BrandTotal”).

I have been asked to evaluate the technologies and practices at issue in this case as described in Section VI of this Report.

I expect to testify before the U.S. District Court for the Northern District of California regarding my findings and opinions set forth in this Expert Report and Opinion (“Report”), as well as for any further matters in this action for which I have or will submit expert analysis or opinions. I reserve the right to rely on demonstratives at trial. All opinions within this report are made within a reasonable degree of scientific and/or technical certainty. I reserve the right to supplement or amend this Report or my opinions and conclusions as necessary and if I am presented with new information.

II. Scope of Evaluation and Work

I have been retained by Wilmer, Cutler, Pickering, Hale, and Dorr LLP (“WilmerHale”), counsel for Meta Platforms, Inc. (“Meta”), to conduct an evaluation of BrandTotal’s technology and practices (as set forth in Section VI) and to render an expert opinion regarding the following matters.

I have been asked to evaluate the cybersecurity risks associated with BrandTotal’s technologies and data scraping practices (as set forth in Section VI) as they pertain to interactions with Meta’s computer systems, platforms, products, and other technologies, as well as the cybersecurity harms that may flow from those risks.

My analysis is limited to these questions and any associated questions which, in my expertise and professional judgment, are required to address these questions. My analysis is not a comprehensive cybersecurity analysis of Meta or any of its systems.

III. Qualifications

I am an internationally-recognized expert in cybersecurity and cybercrime. I hold a Ph.D. in Information Management and Systems, an M.A. in Political Science, and a J.D., all from the University of California, Berkeley. I hold undergraduate degrees in Computer Science and Government and Politics from the University of Maryland. I am a licensed attorney in Connecticut, New York, the District of Columbia, and Texas. Full details of my educational background and training are listed in my curriculum vitae, attached as Exhibit A to this report.

I am currently on research leave from my post at the University of Pittsburgh,¹ where I hold an appointment while on leave as Associate Research Professor of Law and Assistant Research Professor of Computing & Information. I am the Founder and Faculty Director of the CyREN Laboratory, which specializes in developing generalizable datasets regarding adversaries' methods of compromising information systems. I also am an Affiliated Fellow of the Information Society Project at Yale Law School, and for the 2021-2022 academic year am a Visiting Faculty Fellow of the University of Nebraska Governance and Technology Center. I have published and presented extensively in academic journals and conferences on the subjects of cybersecurity and cybercrime and related topics. Full details of my academic appointments are listed in Exhibit A.

I have served on the Advisory Boards of several multi-national technology firms and was a co-founder and Advisory Board member of a cybersecurity non-profit. Before joining the University of Pittsburgh, I held faculty positions at the University of Connecticut School of Law and the University of Maryland Department of Computer Science. I also practiced cybersecurity and privacy law with Hogan & Hartson (now Hogan Lovells) in Washington, DC, and worked for many years in various positions in the information technology industry. Full details of my professional industry experience are listed in Exhibit A.

I have testified before and advised several agencies and entities of the United States Government and other allied nations on issues of cybersecurity and cybercrime, including testimony before the United States Congress and work with the U.S. Department of Defense. A list of these and related professional activities is available in Exhibit A. In accordance with Federal Rule of Civil Procedure 26(a)(2)(B)(v), I state that I have testified at trial or by deposition as an expert witness in the following matters within the past four years:²

¹ While on research leave, I am working on a distributed computing project known as the Obnestic Project, based in Dallas, TX with collaborators in Seoul, Korea. The work involved in this project is noted on my curriculum vitae.

² As of the date of this Report. Out of an abundance of caution of compliance with Rule 26, I also note that I testified before an arbitration panel as an expert witness in 2019 in the matter of *The Estate of Marylou Schwartz & the Estate of James William Schwartz v. Cellco Partnership d/b/a Verizon Wireless, NYNEX Long Distance d/b/a Verizon Enterprise Solutions & Verizon Communications, Inc.*, American Arbitration Association Case No. 01-17-007-0523. I was not deposed in that matter.

- *Orbital Engineering, Inc. v. Jeffrey J. Buchko*, No. 2:20-cv-00593 (W.D. Pa., pending).

IV. Evaluation Basis and Compensation

The opinions expressed in this Report are based on my expertise in the fields of cybersecurity and cybercrime and my evaluation of the documentation and technical materials presented to me, and the conclusions of Mr. David Martens as set forth in Section VI of this Report. A list of the information relied upon is provided in Appendix B. Appendix B includes the documents and other technical materials provided by counsel upon which I relied, but does include external references such as scientific, technical, or other publications or material which are publicly available. When such publicly available materials are directly relied upon, cited, or quoted in this Report, a footnote will appear with the reference describing the source in a manner reasonably expected to allow others to access that resource.³

My rate of compensation for this matter is \$750/hour (with an optional “day rate” for testimonial days of \$2500/day which may be selected in advance),⁴ plus any direct expenses incurred. My compensation is based solely on the time spent preparing this report and any associated testimony in future proceedings and in no way affects my opinions in this matter. My compensation is independent of and does not depend on any outcome in this matter. As is my usual practice, I performed an initial analysis of the matter free of charge before agreeing to this engagement.

³ Some technical standards are published, but reproduction limited by copyright restrictions, and I make no representations regarding the costs associated with those materials or my ability to provide them without charge. For example, the International Organization for Standardization (ISO), which publishes the ISO 27000 series pertaining various cybersecurity standards, charges a fee for copies of many of the standards in that series. See generally <https://www.iso.org/isoiec-27001-information-security.html> and <https://www.iso.org/search.html?q=27000>.

⁴ For the avoidance of doubt, the rate charged for a “testimonial day” only defaults to the “day rate” for trial testimony days (given the inherent uncertainties of trial planning). Deposition or other testimonial acts other than trial testimony are billed at the hourly rate unless prior arrangements are made before the day(s) in question. To the extent the decision is within my control, it is my usual and customary practice to grant reasonable requests for the “day rate” option. An example of an “unreasonable” request would be for a day rate that contemplated 12 hours of actual availability in a given day. In calculating “availability” for this purpose (other than trial days), all hours the requesting party asks that I be available – regardless of whether or not I actually am giving testimony during those times – are included.

V. Standards and Methodology

In general terms, I employ the sum of my knowledge and expertise in the field of cybersecurity when conducting an evaluation of the type requested for this Report.

To the extent my analysis relies upon knowledge of the function of BrandTotal's technology not stipulated to by the parties, admitted by BrandTotal, or testified to by BrandTotal's Fed. R. C. P. 30(b)(6) deponents, I generally rely upon the conclusions of the Martens Report, as set forth in Section VI of this Report. Except as otherwise noted, I have not conducted independent analysis of BrandTotal's technology. My opinions and conclusions might change if information in the Martens Report were to change, if the other stipulations or admissions in this case were ordered revised or updated by the Court, or if new information regarding BrandTotal's technologies and practices became available to me.

Additionally, as is common more generally within the field of cybersecurity, many of the technologies involved are what would colloquially be described as "emerging," and as such may require the evaluation of new technologies, implementation, data, methods, risks, or other scientific or technical matters for which limited scientific evidence may yet exist. In such instances, I apply standards and methodologies which, in my judgment, education, training and professional experience, most likely represent the current state of how the field of cybersecurity or computing and information technology more generally would be likely to approach such an emerging question.

VI. Assumed Conduct of BrandTotal

I have not been asked to opine on the operation of BrandTotal's technologies or systems, nor have I conducted an independent analysis of the relevant evidence. Instead, for purposes of this Report, I have been instructed to assume that BrandTotal's technologies engage in the following conduct as described in the Martens Report. Collectively, I refer to these technologies and the conduct in which I assume they engage as "BrandTotal's Assumed Conduct."

The following language (in this Section VI) from the Martens Report describes Mr. Martens' opinions and conclusions with respect to BrandTotal's technologies and practices. I have not independently evaluated the evidence relating to BrandTotal's systems and practices to evaluate the technical basis for his conclusions, nor is that within the scope of what I was asked to evaluate for this case. Instead, I have been asked to review his report and assume that his descriptions of BrandTotal's technologies and practices (as detailed in his report and excerpted below) are accurate, and on that basis, to offer my opinions regarding the cybersecurity risks

and harms associated with BrandTotal's Assumed Conduct, based upon my experience, expertise, and knowledge of the field of cybersecurity.

A. Methods of Data Collection

■ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

⁵ Martens Report § 4.7.1.

⁶ *Id.*

⁷ *Id.*

⁸ *Id.*

⁹ *Id.*

¹⁰ Martens Report §§ 7.4, 9.4.

¹¹ Martens Report §§ 7.3.1, 7.4, 9.3.1, 9.4, 10.3.1, 10.4.

¹² Martens Report § 4.7.2.

Meta Platforms v. BrandTotal
Expert Report and Opinion of Dr. David Thaw

No. 3:20-CV-07182-JCS (N.D. Cal.)
Page 6 of 26

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

¹³ *Id.*

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ Martens Report §§ 7.3.2, 7.4, 8.3.1, 8.4, 9.3.2, 9.4, 10.3.2, 10.4.

¹⁸ Martens Report § 4.7.3.

¹⁹ *Id.*

²⁰ *Id.* § 6.4.

²¹ *Id.*

²² Martens Report §§ 4.10, 6.2, 8.5, 9.5, 10.5.

Meta Platforms v. BrandTotal
Expert Report and Opinion of Dr. David Thaw

No. 3:20-CV-07182-JCS (N.D. Cal.)
Page 7 of 26

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

²³ Martens Report §§ 4.10, 7.5, 8.5, 9.5, 10.5.

²⁴ Martens Report §§ 4.7.1, 4.10, 7.5, 9.5, 10.5.

²⁵ Martens Report §§ 4.10, 7.5.

²⁶ Martens Report § 5.1.

²⁷ Martens Report §§ 4.10.1, 4.14.8, 7.5, 7.7.4.

²⁸ Martens Report §§ 4.14.2, 6.6.3, 7.7.1, 10.7.2.

those communications are actually originating from Anonymous Story Viewer and Story



H. Failure to Distinguish Between Multiple Users of a Shared Computer

Because early versions of BrandTotal's browser extensions such as UpVoice 2019 and related extensions ran in the background during browser sessions and did not turn their collection mechanisms on or off in response to changes in who was actually using a browser, it is inevitable that in cases where multiple individuals share the use of a single computer browser, UpVoice 2019 and related browser extensions collected data from individuals without their knowledge.³⁷

²⁹ Martens Report § 7.7.1; *see also id.* § 10.7.2 (Social One and Phoenix), *id.* § 6.6.3 (server-side direct collection).

³⁰ Martens Report § 6.6.2.

³¹ Martens Report § 4.14.3.

³² *Id.*

³³ Martens Report § 6.4.

³⁴ Martens Report § 6.6.1.

³⁵ *Id.*

³⁶ *Id.*

³⁷ Martens Report § 4.14.5.

I. Use of Hash Functions

Hash functions are a class of software algorithm that produce a fixed-length output from a variable-length input.³⁸ Hash functions can incorporate a “salt” to provide enhanced security relative to results generated without a salt.³⁹ A salt is a string added to information input to a hash function.⁴⁰ Salts can either be static or dynamic, with dynamic salts providing a much higher degree of security – especially against reverse engineering of input information by an application developer.⁴¹ A static salt, such as a fixed set of characters, remains constant at all times.⁴² A dynamic salt, such as a random string, is modified on a time interval.⁴³ Early versions of UpVoice 2019 employed a static salt.⁴⁴

[REDACTED]

VII. Relevant Cybersecurity Principles

This Section provides an overview of certain general principles in cybersecurity and related fields helpful to understanding my analyses and opinions in this Report. It also presents the development of terminology to describe certain such general principles where, based on my expertise, experience, and training, I believe supplying such descriptive terms for the purposes of this Report will simplify the process of my explaining otherwise lengthy or complex technical terms in context.

A. Automated Information Collection

Automated Information Collection (“AIC”), as used in this Report, describes the general concept of technologies and or processes by which data is gathered and extracted from a target resource using computer code or other technology that automates that collection and extraction.

For virtually all resources, preventing system disruption or interference with resource availability is a concern. While the degree of concern will vary based on the specifics of the

³⁸ Martens Report § 4.14.7.

³⁹ *Id.*

⁴⁰ *Id.*

⁴¹ *Id.*

⁴² *Id.*

⁴³ *Id.*

⁴⁴ Martens Report § 9.7.1.

⁴⁵ Martens Report § 4.14.4.

design, limitations on AIC are common (if not near-universal) for this reason if no other. This is because without such limitations, while a single or even few instances of AIC might not disrupt the system, in many cases even the adoption of AIC by a small proportion of “users” could disrupt the system.

Restrictions on AIC are commonplace throughout the information technology industry. For example, the resource Wikipedia provides a web interface and mobile app for users to read articles on a wide range of topics (similar to, but a broader conception than, a traditional encyclopedia). It is a resource which is freely available, collectively developed and edited, and has experienced remarkable success in developing accurate information about technical topics. Wikipedia expressly places no limits on how much information users may read.⁴⁶ However, even Wikipedia – which describes itself as facilitating widespread knowledge dissemination – nonetheless places limits on the automated collection of its data, effectively reserving the right to prohibit AIC generally and expressly prohibiting certain examples thereof, noting in relevant part that users are subject to the conditions of:

no harm – [users may] not harm [Wikipedia’s] technology infrastructure [and] may not engage in [certain] activities on [Wikipedia] . . . these include: . . . Engaging in Disruptive and Illegal Misuse of Facilities [such as] . . . Engaging in automated uses of the site that are abusive or disruptive of the services and have not been approved by the Wikimedia community [or] Disrupting the services by placing an undue burden on a Project website or the networks or servers connected with a Project website [or] Disrupting the services by inundating any of the Project websites with communications or other traffic that suggests no serious intent to use the Project website for its stated purpose.⁴⁷

Similar prohibitions can be found on public Internet resources of all types maintained by governments, other public sector and non-profit organizations, and private-sector for-profit entities across the organizational spectrum.⁴⁸ Many such prohibitions are phrased broadly as

⁴⁶ Wikipedia Terms of Use, https://foundation.wikimedia.org/wiki/Terms_of_Use/en (last accessed Jan. 12, 2022) (noting in relevant summary part that “[users] are free to: Read and Print [Wikipedia] articles and other media free of charge” and leading the more specific contractual Terms of Use with the vision statement “Imagine a world in which every single human being can freely share in the sum of all knowledge. That’s our commitment.”).

⁴⁷ *Id.*

⁴⁸ See, e.g., restrictions on automated collection in place by the New York Times (*infra* n. 52), YouTube (<https://www.youtube.com/static?template=terms>, noting that users “are not allowed to ... access the Service using any automated means (such as robots, botnets or scrapers) except (a) in the case of public search engines, in accordance with YouTube’s robots.txt file; or (b) with YouTube’s prior written permission”), Twitter (<https://twitter.com/en/tos>, noting that users may not “access or search or attempt to access or search the Service by any means (automated or otherwise) other than through our currently available, published interfaces that are provided by Twitter ... unless you have been specifically allowed to do so in a separate agreement with Twitter” and noting that “scraping the Service without to prior consent of Twitter is expressly prohibited”), restrictions in place on the official websites of the United States Congress (<https://www.loc.gov/legal>, noting “We reserve the right to block IP addresses that fail to honor our websites’ robot.txt files, or submit requests at a rate that negatively impacts service delivery to patrons. Current guidelines recommend that software programs submit a total of no more than 10 requests per minute to our applications, regardless of the number of machines used to

limitations on “disruption,” “interruption,” or the introduction of “harmful” activities/code to the site, as opposed to limitations on AIC alone.⁴⁹ This is in part to ensure that new or unanticipated tactics, techniques, or procedures of adversaries do not fail to be prohibited.

Indeed, BrandTotal’s own website “Service Terms and Conditions” include, in relevant part, the following restrictions both on AIC specifically and service interruption generally:

5.1. Restrictions on Use of the Site. You shall not, and shall not allow any third party to: . . . (iii) disrupt servers or networks connected to the Site; (iv) use or launch any automated system (including without limitation, “robots” and “spiders”) to access the Site; and/or (v) circumvent, disable or otherwise interfere with security-related features of the Site or features that prevent or restrict use or copying of any Content or that enforce limitations on use of the Site.

submit requests.”), the Electronic Frontier Foundation (<https://www.eff.org/security>, noting “Do not DDoS or otherwise disrupt, interrupt or degrade our internal or external services”), CNN (<https://www.cnn.com/terms0>, noting among other related prohibitions that users “agree not to interfere with or disrupt the Site or the servers or networks connected to the Site, or disobey any requirements, procedures, policies or regulations of networks connected to the Site”), FOX News (<https://www.foxnews.com/terms-of-use>, noting that FOX may “may also impose limits on certain features and services offered on the Site or restrict your access to parts or all of the Site without notice or liability”), the City and County of San Francisco (<https://sf.gov/privacy-policy>, noting that “We monitor network traffic to identify unauthorized attempts to upload or change information or to otherwise cause damage to the site. Anyone using this website expressly consents to such monitoring” and “We take appropriate security measures to protect unauthorized access, alteration or destruction of data”), the City of New York (<https://www1.nyc.gov/home/terms-of-use.page>, noting that users may not “use NYC.gov to upload any content that contains a software virus, “Trojan Horse” or any other computer code, files, or programs that may alter, damage, or interrupt the functionality of NYC.gov or the hardware or software of any other person who accesses NYC.gov”), the Democratic National Committee (<https://democrats.org/terms-of-service/>, noting that users may not “use the Services other than for their intended purpose or in any manner that could interfere with, disrupt, negatively affect or inhibit other users from fully enjoying the Services or that could damage, disable, overburden, or impair the functioning of the Services in any manner”), the Republican Party of Texas (<https://texasgop.org/terms-and-conditions/>, noting that users may not “post, upload, transmit, distribute, store, create, or otherwise publish to or through the Sites” . . . “User Content that impersonates any person or entity or otherwise misrepresents your affiliation with a person or entity” . . . or . . . “Viruses, corrupted data or other harmful, disruptive or destructive files”), and L’Oréal USA (<https://www.loreal.com/en/usa/pages/group/term-of-use-usa/>, noting that users may not “upload, post, e-mail, or otherwise transmit any material that contains software viruses or any other computer code, files, worms, logic bombs or programs designed or intended to interrupt, disable, damage, destroy, or limit the functionality of the Site or any computer software or hardware or telecommunications equipment or any other similarly destructive activity [or] obtain unauthorized access to any system, data, password or other information [or] interfere with or disrupt the Site or servers or networks linked to the Site, or disobey any requirements, procedures, policies, or regulations of networks linked to the Site”).

⁴⁹ Meta prohibits both AIC and other disruptive technologies. The Facebook Terms of Service prohibit “access[ing] or collect[ing] data . . . using automated means (without [Meta’s] prior permission)” as well as “upload[ing] viruses or malicious code or do[ing] anything that could disable, overburden, or impair the proper working or appearance of [Meta’s] Products.” Facebook, *Terms of Service*, <https://www.facebook.com/terms.php> (last accessed January 12, 2022). The Instagram Terms of Use prohibit “collecting information in an automated way without [Meta’s] express permission” as well as “do[ing] anything to interfere with or impair the intended operation of the Service.” Instagram, *Terms of Use*, <https://help.instagram.com/581066165581870> (last accessed January 12, 2022).

5.2. Restrictions on Use of the Software. You shall not, and shall not allow any third party to: . . . (iv) use any automated means to access or use the Software, nor circumvent or disable any security or technological features of the Software; (v) use, send, upload, post, transmit or introduce any device, code, routine or other item (including without limitation bots, viruses, worms, and Trojan horses) that interferes (or attempts to interfere) with the operation or integrity of the Software, nor any content that is unlawful, infringing, defamatory, deceptive, obscene fraudulent, harassing, pornographic, or abusive; (vi) use the Software to design or develop any competing product or service that competes with the Software; (vii) use the Software for any unlawful or fraudulent purpose, to breach these Terms, or infringe or misappropriate any third party intellectual property, privacy, or publicity right; (viii) take any action that imposes or may impose, as determined in BrandTotal's sole discretion, a disproportionately large load of incoming requests on the Software infrastructure; or (ix) violate or abuse password protections governing access to the Software.⁵⁰

The specifics of the reasons why a resource operator might have cause to limit the total quantity or rate of data access vary by context. For an open-knowledge distribution non-profit like Wikipedia, for example, the greatest concern may be system stability.⁵¹ By contrast, for a news organization like the New York Times, the primary concern may be protecting adequate subscriber revenue to sustain journalistic operations.⁵²

Such restrictions play important roles not only in maintaining system availability and stability, but also in enabling more technologically-sophisticated applications, which require the transmission of information not intended for direct user consumption but required as “behind-the-scenes” elements⁵³ to enable those elements intended for direct user consumption.

In the Wikipedia case, for example, the system design assumes a certain number of (human) users per unit time. An “AIC user” can easily access many orders-of-magnitude more information in that same unit time than can a human user. This disrupts the assumptions involved in system design and, accordingly, can result in partial or even total disruption of the system depending on the number of AIC users concurrently accessing the system. If one AIC user scrapes information at a rate equivalent to 10,000 times the average human user (a

⁵⁰ See BrandTotal.com, Service Terms and Conditions, https://privacy.brandtotal.com/service_terms.pdf (last accessed Jan. 12, 2022).

⁵¹ See supra n. 46-47.

⁵² See The New York Times Terms of Service § 4 Prohibited Use of the Services, <https://help.nytimes.com/hc/en-us/articles/115014893428-Terms-of-service#4> (last accessed Jan. 12, 2022) (prohibiting in relevant “[the use of any] robots, spiders, scripts, service, software or any manual or automatic device, tool, or process designed to data mine or scrape the Content, data or information from the Services, or otherwise access or collect the Content, data or information from the Services using automated means”).

⁵³ Modern web applications, mobile apps, and similar technologies inherently communicate significantly more information from the app “server” (host) device to the “user” (client) device than is displayed to the user. This additional information is technologically necessary for the user’s app or browser to render the information intended for user display.

modest estimate of AIC capabilities in the Wikipedia context), then 100 AIC users would be equivalent in system load to 1,000,000 concurrent human users.

B. Private vs. Public Areas of Meta's Computer Systems

Most computing and information systems store data with some level of access control. This means that there exists some amount of data stored by the system which is designed to be unavailable to some or most users of the system, where such availability is enforced by cybersecurity controls. These cybersecurity controls generally fall under the category of access controls, and employ technologies including usernames, passwords, and other types of identification and/or authentication credentials⁵⁴ (including access tokens and cookies), among other methods.

In the context of social media platforms, like Facebook and Instagram, the privacy features of the network itself further complexify these distinctions. However, for the purposes of the present analysis, one distinction is key – those areas of the Facebook and Instagram platforms which are “publicly available” (i.e., for which no authentication is required) as compared to those areas of the platforms where at least some authentication is required.

1. “Publicly” Available Areas of Meta Systems

Publicly Available Areas of Meta-owned systems are those areas for which no special authentication is required as a condition of access. Note a key distinction here – no *special* authentication is required here. The distinction refers to the fact that a system operator might well implement some form of access control mechanism to, for example, restrict access to those areas only to “human” users (e.g., through the use of a “prove you’re a human” technology like a CAPTCHA⁵⁵ or similar technology). Such a restriction is not designed to limit *which* human(s) can access the system, as was the case with early computing authentication systems,⁵⁶ but is designed to ensure that the agent accessing the system is, in fact, a human agent. Regardless of whether or not a system operator restricts access to Publicly Available Areas only to humans, or permits non-human agents to access those resources as well, the key distinction remains – the system operator is not seeking to restrict accessed based on *which* human is attempting to utilize a resource and/or retrieve information.

⁵⁴ Identification refers to an assertion of identity, the equivalent of a human saying “my name is David Thaw.” By contrast, authentication refers to the process of confirming that an agent claiming an identity, authorization, or similar system privilege is, in fact, the agent they claim to be and/or is entitled to the authorization or privilege that they claim.

⁵⁵ CAPTCHA is an acronym for the term “Completely Automated Public Turing test to tell Computers and Humans Apart” which is a security access control mechanism designed to permit humans easily to respond to a challenge, but make it extremely difficult for an automated (computing) system to do so. See, e.g., Google, What is CAPTCHA, <https://support.google.com/a/answer/1217728?hl=en> (last accessed January 12, 2022). Such systems have varying rates of failure, and are often problematic for human users, but for certain purposes serve as an effective mitigation technique.

⁵⁶ See generally Robert Morris & Ken Thompson, *Password Security: A Case History*, 22 COMM. ACM 594 (1979).

An example of a Publicly Available Area of Meta-owned systems is the Facebook log-in page.⁵⁷

2. Non-Publicly Available (Private) Areas of Meta Systems (the “Privacy Sphere”)

Certain areas of Meta-owned systems or products and the data contained within those areas is designated, either by Meta directly or by the users through settings provided by Meta, as having some limitation on the scope of users who are able to access those resources or view that data.

A user’s Facebook News Feed is non-public. Facebook’s Help Center describes News Feed as

the constantly updating list of stories in the middle of your home page. News Feed includes status updates, photos, videos, links, app activity and likes from people, Pages and groups that you follow on Facebook.⁵⁸

This essentially is a collection of posts, including sponsored posts, that appear on a user’s own Facebook home page based on that user’s actions on the platform, including the people, Pages, and groups that they follow.⁵⁹ A user’s News Feed is viewable only through that user’s log-on credentials.⁶⁰

The effect of this distinction is that Meta maintains “areas” of its Facebook and Instagram platforms that are not accessible without being an authenticated user with specific credentials, and which contains data that Meta and/or Meta’s users designate with expectations that Meta systems will enforce access protections against said data. I refer to these portions of Meta’s systems, and the data so designated within them, as part of the Non-Publicly Available “Privacy Sphere.”

C. User Authentication

Basic principles of authentication are cornerstones of cybersecurity – addressing the question of what actor is utilizing a given resource.⁶¹ The ability for a system operator to regulate activities on its system is essential to cybersecurity. From the perspective of cybersecurity as a

⁵⁷ See Facebook, *Log In or Sign Up*, <https://www.facebook.com/> (last accessed January 12, 2022).

⁵⁸ Facebook, *How News Feed Works*, <https://www.facebook.com/help/1155510281178725> (last accessed January 12, 2022); Facebook, *Your Home Page*, https://www.facebook.com/help/753701661398957/?helpref=hc_fnav (last accessed January 12, 2022). But note that while these elements are within the Privacy Sphere by design, some objects within those elements (e.g., a given post or picture) can be set by the user to “Public”, placing that object outside the Privacy Sphere.

⁵⁹ *Id.*, see also Facebook, *Ad Preferences*, <https://www.facebook.com/help/109378269482053/?helpref=related> (last accessed January 12, 2022).

⁶⁰ Facebook, *Your Home Page*, https://www.facebook.com/help/753701661398957/?helpref=hc_fnav (last accessed January 12, 2022).

⁶¹ See, e.g., Steven M. Bellovin, THINKING SECURITY Ch. 7 (noting that “[a]uthentication is generally considered to be one of the most basic security principles. Absent bugs – admittedly a very large assumption – authentication effectively controls what system objects someone can use. In other words, it’s important to get authentication right.” at 107).

scientific and technical matter, operators of systems must be able to prohibit activity which disrupts, disables, damages, or interferes with their system operation, including the ability to limit or deny access to users who engage in such activity.

Many modern web applications, including Facebook and Instagram, use authentication credentials (e.g., browser cookies or access tokens⁶²) to allow users to remain “logged in” to a system on their own personal computers without having to re-enter their usernames and passwords. Nearly all modern web applications use some form of session-length authentication token like this to ensure the user does not have to re-enter their username and password each time they navigate throughout the application. Many, including both Facebook and Instagram, include authentication credentials which persist beyond a single session.

VIII. Analysis of Risks And Harms Associated With BrandTotal’s Assumed Conduct

This Section discusses the cybersecurity risks and associated possible harms generally created by BrandTotal’s Assumed Conduct. Risk management is a key element of cybersecurity, so in analyzing the potential harm of a technology one must not only consider the actual results which have happened thus far, but also the potential risks created by a technology or process in the individual case and the general case if that technology or process is permitted to occur at scale. This Section analyzes the potential risks associated with BrandTotal’s Assumed Conduct, as well as those risks that would follow if entities like Meta were not allowed to prohibit the use of such technologies and practices. Based on those risks, this Section then analyzes and opines on the types of harm associated with those risks.

A. System Impairment

Failing to have restrictions on AIC creates the risk of system disruption. This can lead both to the lack of system availability (a classic case of cybersecurity risk⁶³) or other unintended or unexpected system operation, which – depending on the context – could create a variety of different risks. In both instances, it is the possibility of the risk that the restriction seeks to

⁶² The Martens Report uses the term “access tokens” to refer to certain credentials maintained in “token” form (i.e., single, usually unique, stateful information used both for identification and authentication purposes) other than browser cookies. For the purposes of my Report, I assume this usage of “access tokens” to be a general term encompassing all token-based authentication methods described in the Martens Report other than browser cookies and, collectively, that together “cookies” and “access tokens” refer to all relevant authentication credentials.

⁶³ The concepts of “confidentiality, availability, and integrity” (often referred to as the “CIA model”) are fundamental general categories often used in evaluating system security from a theoretical standpoint. The term is widely used throughout the industry today, but traces back to early computer security theory. See Zella G. Ruthberg and Robert G. McKenzie (eds.), U.S. DEP’T OF COMMERCE, NAT’L BUREAU OF STANDARDS, AUDIT & EVALUATION OF COMPUTER SEC. (NBS Spec. Pub. 500-19) at 11-3 (Oct. 26, 1977) *available at*: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nbsspecialpublication500-19.pdf> (presenting a key early historical example of the use of this theoretical framework in describing the “[o]bjectives of a typical security audit”).

prevent because, as discussed below, many potential (and likely) harms flow from the existence of those risks. A primary defense against such risks is to prohibit the conditions – AIC and targeted or specific system impairment or interference – that create the risks in the first instance.

1. Impairment via System Overload (Denial-of-Service)

System overload is a common risk in which the rate or load of requests made to a system exceed that system's capacity to respond to requests. The result is that the system will fail to respond to some (otherwise-valid) requests, a condition sometimes described as "denial-of-service" since the system's failure to respond to legitimate users' requests as a result effectively "denies" those users (otherwise authorized) access. This is an example of the classic cybersecurity risk of impaired system availability.

In the Wikipedia hypothetical discussed in Section VII.A above, a mere 100 AIC users could become equivalent to one *million* concurrent legitimate Wikipedia users. If each organization implementing AIC were to deploy 1,000 AIC "users" operating on a daily basis, and 50 organizations operated in that space, the result would be the equivalent of an additional 500,000,000 concurrent Wikipedia users – or approximately 16% of the world's population concurrently using Wikipedia. For comparison, as of September 2021, TikTok – which surpassed Google in 2021 as the most-visited domain – only had approximately 1 billion monthly active users.⁶⁴

Stated differently, under this hypothetical, unchecked AIC could result in Wikipedia being subject to an approximate *daily user load* roughly equivalent to half the *monthly user load* of the world's most-visited domain in 2021. As a result, Wikipedia would be limited in its ability to respond to legitimate non-AIC data requests.



to be the official measure of the social world and the go-to brand intelligence platform for everything social advertising. We want to be the one source of truth that indexes,

⁶⁴ See Jessica Bursztynsky, *TikTok says 1 billion people use the app each month*, CNBC (Sept. 27, 2021), <https://www.cnbc.com/2021/09/27/tiktok-reaches-1-billion-monthly-users.html>.

⁶⁵ See *supra* Section VI.G.

⁶⁶ See *id.*

categorizes, benchmarks, and measures social advertising in every brand category so marketers can make decisions with data, not feelings.⁶⁷

It is my analysis and opinion that it is highly likely that BrandTotal's Assumed Conduct could interfere with the operation of Meta's systems.⁶⁸

Based on my experience and expertise in the field of cybersecurity, entities with the incentives, stated goals, and access to scalable technological resources like BrandTotal are highly likely to engage in AIC at levels capable of interfering with the operation of even large-scale systems like those operated by Meta. Furthermore, if Meta is not able to prohibit such AIC activities and effectively enforce such prohibitions, it is my opinion that it is highly likely other actors could and would enter this industry and AIC would rapidly become commonplace. While system owners might be able to technologically manage the effects of a single or very few actors engaging in AIC, it would rapidly become cost-prohibitive (and potentially technologically impractical) to manage the effects of AIC coming from 100 actors, let alone 1000 or 10,000 actors. Organizations like Meta are extremely attractive targets for AIC, ranging from those actors who believe themselves well-intentioned and acting with public goals (e.g., public interest organizations), those with economic goals (e.g., third-party analysis services like BrandTotal), to those actors with unlawful and/or malicious intentions (e.g., organized crime and foreign intelligence services).

It is my opinion that if organizations are not able to prohibit AIC and effectively enforce such prohibitions, the scale of AIC activities will rapidly increase and overwhelm the system capacity even of organizations like Meta – let alone other, less technologically-sophisticated organizations (e.g., public institutions and non-profit organizations) providing services via the public Internet – such that the provision of these services as construed today will become impractical. While I cannot opine with precision how the marketplace would respond to such a fundamental shift in the enforceability of basic cybersecurity principles, it is my opinion that absent extremely strict authentication protocols (e.g., requiring full human-specific authentication for *all* access to *all* resources on the public Internet⁶⁹) the public Internet as we know it today would significantly change.

2. Targeted or Specific Impairment/Interference

Impairment and other interference is not limited only to overloading system capacity. It also can be targeted or specific, designed to alter or change the way in which a system operates. For example, if an actor can gather information regarding the preferences and activities of an

⁶⁷ See BrandTotal, *Our Company*, <https://www.brandtotal.com/about/our-company> (last accessed January 12, 2022).

⁶⁸ For the purposes of this analysis, I assume the information provided to me in Section VI and BrandTotal's self-described goals. To achieve those goals, a very significant amount of information would need to be collected across Meta's platforms. While the specifics would of course vary, the implied scale and scope in BrandTotal's self-professed goals are inherently of an order-of-magnitude sufficient to impact Meta's systems.

⁶⁹ Which, in relevant part, *would* constitute a fundamental change in the public Internet as we know it today.

algorithmic recommender system, and gain access to that system (e.g., through impersonating users on that system), that actor then could use this information to manipulate the content displayed to users on that system.⁷⁰

As discussed in Section VI, BrandTotal's Assumed Conduct directly accesses or otherwise obtains information from Meta's Privacy Sphere.⁷¹ To the extent such activities reveal information otherwise not available to BrandTotal, and such information is exfiltrated outside Facebook's or Instagram's respective Privacy Spheres, it is my opinion that this risks the disruption of Meta's systems by enabling subsequent targeted attacks based on that exfiltrated information.

The risk of such targeted attacks, described in more detail in the following paragraphs, are enabled by information exfiltrated by BrandTotal's Assumed Conduct which includes demographic, activity, and advertising data from which significant inferences regarding the preferences and activities of a given user can be drawn.⁷² Information of this nature can be used to draw conclusions regarding specific users, specific groups, or aggregations thereof – inferences which can then, in turn, be used by BrandTotal, BrandTotal's customers, or other actors to engage in a variety of economically-harmful, criminally unlawful, or foreign espionage activities as described in Section VIII.D.

The risk of specific or targeted system interference created by this data exfiltration process are not limited to the ways in which the data itself can be used. The *processes* involved in BrandTotal's Assumed Conduct themselves can create the risk of targeted or specific system interference. This is because the ways in which Meta's systems operate are responsive to the activities of the user.⁷³ Thus, for example, Active Collection of the sort engaged in by BrandTotal's Assumed Conduct could not only collect information, but could also be used to *influence future information* displayed to that or other users.⁷⁴ The types of attacks that create these risks are generally referred to as "(data) poisoning attacks"⁷⁵ or "shilling attacks."⁷⁶

Risk in cybersecurity is not just about already-realized harms – indeed, it is most often about identifying (and mitigating) the possibility of *future harm*. In that regard, I have analyzed the harms that would flow from the ability to influence the future content that users see on Meta's

⁷⁰ See, e.g., *infra* n. 75-76 and the discussion those notes reference of data "poisoning" and "shilling" attacks.

⁷¹ See Section VI.A.

⁷² See Section VI.B.

⁷³ See *supra* n. 58 (regarding News Feed) and n. 59 (regarding Ad Preferences).

⁷⁴

⁷⁵ See generally Wenqi Fan, Tyler Derr, Xiangyu Zhao, et al., *Attacking Black-box Recommendations via Copying Cross-domain User Profiles*, 2021 IEEE 37TH INT'L CONF. ON DATA ENG'G 1583 (Apr. 19-22, 2021).

⁷⁶ See generally Shyong (Tony) K. Lam and John Riedl, *Shilling Recommender Systems for Fun and Profit*, WWW '04: PROCEEDINGS OF THE 13TH INT'L CONF. ON WORLD WIDE WEB 393 (May 17, 2004).

platforms (the “risk”) through the types of targeted or specific interference possible as a function of the kind of Active Collection involved in BrandTotal’s Assumed Conduct (the types of technology creating the “risk”). In short, these activities (as discussed above) provide a pathway by which outside actors could influence the content that Meta’s users see, potentially in a surreptitious manner. Furthermore, as discussed in Section VIII.A.1, it is my opinion that it is possible and likely that such other actors could and would enter this industry and AIC would rapidly become commonplace, further magnifying the risk of using AIC to influence the content shown to users.

It is my opinion that if organizations are not able to prohibit AIC of the types described in BrandTotal’s Assumed Conduct, and to effectively enforce such prohibitions, the incentives for actors – particularly organized crime and foreign adversaries – to engaged in large-scale specific and targeted system interference activities with AIC would likely create harm by creating avenues for various forms of information distorting activities. Such activities would, in my opinion, rapidly overwhelm regulators, law enforcement, and the abilities of system owners, effectively rendering services like Facebook and Instagram unusable or rendering it effectively impossible to separate legitimate human activity from financially-motivated specific or targeted AIC-based system interference. Furthermore, because the mechanisms of influencing user content exposure include the mechanisms involved with AIC, if Meta were not permitted to enforce prohibitions against AIC as discussed in Section VIII.A.1, it would be possible to influence content delivery in this manner in a way that would be difficult to distinguish between AIC Meta was “compelled” to permit and specific (automated) attempts to influence user content exposure or forms of information distortion.

It is also my opinion that, under such a scenario, foreign state actors would be highly incentivized to engage in espionage activities likely harmful to the national security of the United States and its allies.⁷⁷

B. Breakdown in Mechanisms of Authentication

The concept of sharing access and authentication credentials in cybersecurity deals with the risks created by permitting users to share such credentials. For the purposes of organization, I group such sharing activities into three categories: (1) “Direct Credential Sharing,” which comprises the risks created when users share their credentials with parties not assigned to such credentials or not authorized to use such credentials; (2) “Indirect Credential Sharing,” which comprises the risks created by technology or processes which cause users unknowingly to provide their credentials to a third party or technology not authorized to make use of those credentials; and (3) “Indirect Access Facilitation,” which comprises the risks associated with users providing access to information or other resources on systems via their credentials (but

⁷⁷ See generally David Thaw, *From Russia With Love*, 59 Hous. L. Rev. (forthcoming 2022), <https://ssrn.com/abstract=3038308>.

without actually providing those credentials) to a third party not authorized to access those systems.

Generally speaking, any form of credential sharing, including Indirect Access Facilitation, creates cybersecurity risks because the authentication mechanisms implemented by the system operator no longer can perform their primary function (i.e., ensuring that the system knows whether or not the user attempting to access a resource is permitted to do so). While the nature of the risks will vary based on the type of authentication mechanism, the specifics of the credential sharing, and the design and purpose of the system, the general principles of authentication are violated when credential sharing occurs except as expressly authorized by the system operator.

Credential sharing, including Indirect Access Facilitation, creates a general risk that the system operator will not be able to accurately assess or distinguish individual human usage of the system from AIC usage or accurately distinguish among users of the system (regardless of whether the system permits humans to have multiple user accounts or permits multiple humans to share a single user account). This risk deals with the general needs of system operators to be able to accurately assess system usage and respond to and address improper, harmful, or unlawful usage of the system.

The cybersecurity harms which flow from this risk are the undermining of general principles of authentication. If organizations are not able to prohibit and effectively enforce prohibitions on credential sharing, fundamental principles of authentication will be undermined. In the individual context, system operators will encounter the types of challenges identified above regarding system management – generally dealing with an inability to determine whether an agent attempting to access a system is permitted to do so. The types of activities BrandTotal's Assumed Conduct comprises creates this risk and realizes the harm flowing from that risk both as to access to resources on Meta-owned systems and as to access to information stored in Meta's Privacy Sphere.

[REDACTED]

[REDACTED]

[REDACTED]

The cybersecurity harms that flow from undermining general principles of authentication are not limited to the individual case. It is my opinion that if system operators are not able to set and enforce authentication principles, additional actors will be incentivized to take advantage of these risks and the ability even of organizations like Meta – let alone other, less technologically-sophisticated organizations (e.g., public institutions and non-profit organizations) providing services via the public Internet – to operate any of their services which depend upon authentication will become impractical. While I cannot opine with precision how the marketplace would respond to such a fundamental shift in the enforceability of basic cybersecurity principles, it is my opinion that the public Internet as we know it today would significantly change.

C. Vulnerability of Exfiltrated Authentication Information

[REDACTED]

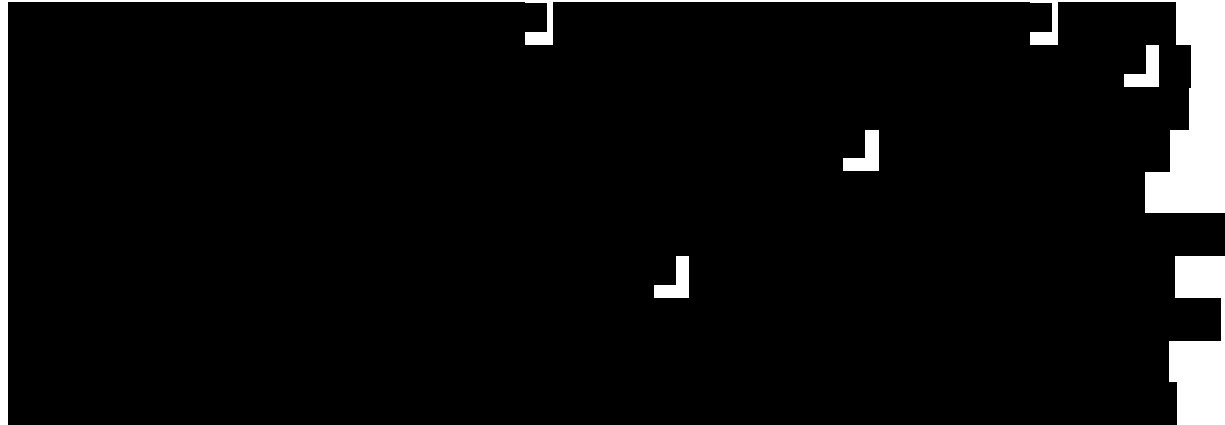
[REDACTED]

D. Vulnerability of Exfiltrated User Data

BrandTotal's Technology has at least the effect – if not also the design – of creating a corpus of data describing individuals' preferences, attributes, or activities (a "User Data Corpus"). BrandTotal's use of insecure hashing algorithms to "anonymize" user IDs, as discussed in Section VI.I, creates the risk that the User Data Corpus created by BrandTotal could be re-associated with identifiable individual users.

⁷⁸ See generally Section VI.

⁷⁹ See Section VI.D.



Moreover, because of the failure of most of BrandTotal's extensions to distinguish between different users of a shared computer,⁸⁶ some of this data is obtained from users who are likely completely unaware that any of their personal data is being collected.

Detailed information regarding the preferences, habits, and activities of individuals is a proverbial "treasure trove" for adversaries to engage in a variety of financial, organized crime (RICO), economic espionage, non-state espionage, or national clandestine espionage activities or other criminal activities.⁸⁷ Additionally, information regarding the practices of advertisers on

⁸⁰

Vol. I at 147:21-152:7.

⁸¹ Dor Dep. Tr. Vol. I 148:10-149:1.

⁸² See Bruce Schneier, *Cryptanalysis of SHA-1*, SCHNEIER ON SECURITY (Feb. 18, 2005), https://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html (last accessed January 12, 2022) (noting that "It's time for us all to migrate away from SHA-1 . . . Luckily, there are alternatives. The National Institute of Standards and Technology already has standards for longer — and harder to break — hash functions: SHA-224, SHA-256, SHA-384, and SHA-512. They're already government standards, and can already be used.")

⁸³ See generally NAT'L INST. OF STANDARDS & TECH. COMP. SEC. RESOURCE CTR., *Research Results on SHA-1 Collisions* (Feb. 24, 2017), <https://csrc.nist.gov/News/2017/Research-Results-on-SHA-1-Collisions> (noting that "NIST deprecated the use of SHA-1 in 2011"), see also shattered.io, <https://shattered.io/> (last accessed January 12, 2022) (cited by NIST in the preceding publication and providing further relevant technical detail).

⁸⁴ Martens Report Section 4.14.7; see also Karve Decl. ¶ 25; Dor Dep. Tr. Vol. I 151:11-152:7.

⁸⁵ See Michael Hill, *Rainbow tables explained: How they work and why they're (mostly) obsolete*, CSO ONLINE (Jul. 6, 2021), <https://www.csoonline.com/article/3623195/rainbow-tables-explained-how-they-work-and-why-theyre-mostly-obsolete.html> (providing a business-targeted explanation of rainbow tables and how salting inputs to a hash algorithm render such attacks significantly less effective).

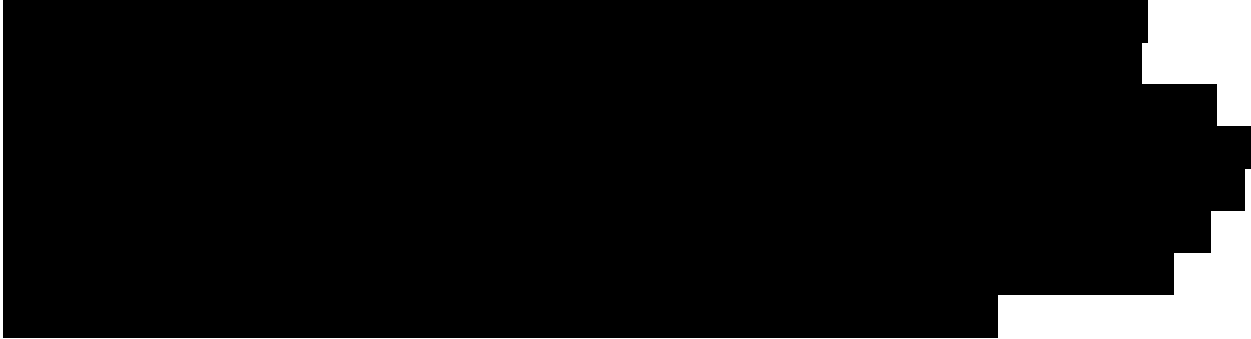



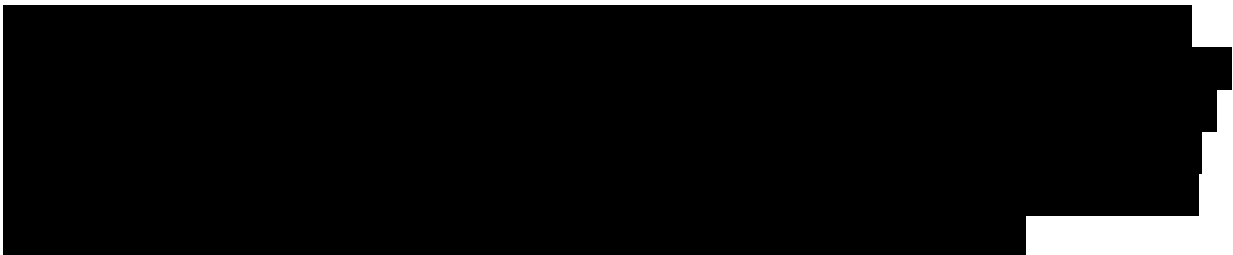
⁸⁶ See Section VI.H.

⁸⁷ For a thorough discussion of the risks of national clandestine espionage by foreign adversaries in the context of election interference, see David Thaw, *From Russia With Love*, 59 HOUS. L. REV. (forthcoming 2022), available at <https://ssrn.com/abstract=3038308> (extensively discussing the ways in which data can be used for election interference by foreign or otherwise unlawful actors). For an overview of the risks of data aggregation by private entities generally, see David Thaw, *Surveillance at the Source*, 103 KY. L. J. 405 (2015), available at <https://ssrn.com/abstract=2512121> (discussing generally the potential harms that can flow from aggregate surveillance by private organizations, and how those differ from government surveillance — a similar analysis among "contemporary" platforms would place Facebook in the role of having incentives to act against the potential harms described, and BrandTotal in the position of lacking incentives to prepare against such harms).

Meta is economically valuable for these actors as well as for lawful market actors. The field of cybersecurity recognizes that organizations have the need to protect certain information (e.g., trade secrets) against unauthorized use or dissemination for economic reasons. It is my opinion that, unless otherwise dictated by law, details regarding the practices of advertisers on Meta would clearly fall within this category of information which the field of cybersecurity would recognize as Meta having an economic interest in protecting.

E. Circumventing Barriers to Access

The idea of circumventing a technological restriction is not a singular concept in cybersecurity, but rather a broad set of activities which generally are grouped together pertaining to attempts to cause a system to permit access to a resource or information when that system ordinarily would not otherwise do so. In this regard the field of cybersecurity distinguishes, for example, inadvertent access to a resource which results from a system design limitation or flaw from access to a resource which results from deliberate development and use of code, practices, or procedures that exploit flaws, technological limitations, or other access control failures.⁸⁸




⁸⁸ To be clear, the field of cybersecurity has mixed opinions on whether inadvertent access resulting from design limitations or flaws *should* be considered unauthorized. However, for the reasons discussed in this Section, that distinction is immaterial when specific code, practices, or procedures are deliberately developed to utilize or “exploit” design limitations or flaws, as is the case here.

[REDACTED]

7

11/11/2016

[REDACTED]



89

⁹⁰ Regev Dep. Tr. 213:9-214:10, 222:21-223:11.

⁹¹ Regev Dep. Tr. 216:6-218:4.

⁹² Facebook, *Terms of Service*, <https://www.facebook.com/terms.php> (last accessed Jan. 12, 2022) (prohibiting the creation of accounts other than for personal use, the use of Facebook by anyone whose accounts have previously been disabled for violating the Terms, and the collection of data “by automated means”).

⁹³ Instagram, *Terms of Use*, <https://help.instagram.com/581066165581870> (last accessed Jan. 12, 2022) (prohibiting the “create[ion of] accounts or access[ing] or collect[ing] information in unauthorized ways,” including “creating accounts or collecting information in an automated way without our express permission”).

Meta Platforms v. BrandTotal
Expert Report and Opinion of Dr. David Thaw

No. 3:20-CV-07182-JCS (N.D. Cal.)
Page 25 of 26

IX. Conclusion

The foregoing report is based on information provided to me as discussed in Sections II, V, and VI and is limited in scope as discussed in Sections I, II, IV, and V. I reserve the right to modify or amend this report if the that information should change or if I receive additional evidence, including but not limited to demonstratives at trial.

I declare, under penalty of perjury, that the foregoing is true and accurate to the best of my knowledge.

DATED: January 12, 2022



David B. Thaw, J.D., Ph.D.

DAVID THAW

University of Pittsburgh • dbthaw@gmail.com • www.davidthaw.com
 3900 Forbes Avenue, Pittsburgh, PA 15260

CURRENT ACADEMIC APPOINTMENTS

University of Pittsburgh, Associate Professor (2019 – Present), Assistant Professor (2014 – 2019)

- **Associate Research Professor of Law**
- **Assistant Research Professor of Computing & Information**

Yale Law School, Affiliated Fellow, Information Society Project (2010 – Present)

University of Nebraska, Visiting Faculty Fellow, Nebraska Governance and Technology Center (2020 – Present)

VISITING AND PREVIOUS FULL-TIME ACADEMIC APPOINTMENTS

Visiting Professor/Visiting Lecturer, Department of American Law – **Hallym University of Graduate Studies**/University of Connecticut Joint Program in American Law (Seoul, Korea) (Summer 2014, Winter 2014-2015, Summer 2015, Winter 2015-2016, Winter 2016-2017, Winter 2017-2018, Winter 2018-2019, Winter 2020-2021)

Adjunct Associate Professor, School of Law – **University of North Carolina** (Spring 2020)

Visiting Professor, Department of Law "Cesare Beccaria," **Università degli Studi di Milano** (Summer 2016)

Visiting Assistant Professor, School of Law – **University of Connecticut** (2012 – 2014)

Research Associate, Department of Computer Science – **University of Maryland** (2011 – 2012)

Visiting Postdoctoral Fellow, Information Society Project – **Yale Law School** (2008 – 2010)

EDUCATION

Ph.D. Information Management and Systems, May 2011 – **University of California, Berkeley**
 Dissertation: *Characterizing, Classifying, and Understanding Information Security Laws and Regulations: Considerations for Policymakers and Organizations Protecting Sensitive Information Assets*
 Advisors: Deirdre K. Mulligan, Pamela Samuelson, Todd LaPorte

J.D. Berkeley Law, May 2008 – **University of California, Berkeley**

M.A. Political Science, May 2004 – **University of California, Berkeley**

B.A. Government and Politics with High Honors, May 2003 – **University of Maryland, College Park**

B.S. Computer Science with Honors, May 2003 – **University of Maryland, College Park**

(course information and related teaching detail appear on final page)

BOOKS

- CYBERSECURITY: AN INTERDISCIPLINARY PROBLEM (interdisciplinary instructional and reference text covering topics in cybersecurity, cybercrime, cyber conflict, and associated regulatory topics for lawyers, scientists, engineers, policymakers, and business leaders) (with Gus Hurwitz, Charlotte Tschider, and Derek Bambauer) (WEST ACADEMIC PUBLISHING, 2021).

PUBLICATIONS

- *From Russia With Love*, 59 HOUSTON LAW REVIEW (forthcoming 2022), <https://ssrn.com/abstract=3038308>.
- *Enhancing Cyber Operations via Artificial Intelligence: Risks, Rewards, and Frameworks*, 54 IEEE COMPUTER 64 (June 2021) (with Joshua A. Kroll and James Bret Michael), <https://ieeexplore.ieee.org/document/9447431>.
- *Bot Contracts*, 62 ARIZONA LAW REVIEW 877 (2020) (with Deborah R. Gerhardt), <http://ssrn.com/abstract=3533517>.
- *Rebooting Congressional Cybersecurity Oversight*, Center for a New American Security: Paper Series on Congressional Oversight (2020), <https://www.cnas.org/publications/reports/rebooting-congressional-cybersecurity-oversight> (with Carrie Cordero).
- *Administrative Truth: Comments on Cortez's Information Mischief*, 94 CHICAGO-KENT LAW REVIEW 607 (2019), <https://ssrn.com/abstract=3389560>.
- *Using Camouflaged Cyber Simulations as a Model to Ensure Validity in Cybersecurity Experimentation*, HICCS 51 Symposia on Cybersecurity Big Data Analytics, Jan. 3-6, 2018 (Big Island, HI) (also accepted for publication in SECURITY INFORMATICS, *Special Issue on Cybersecurity* (forthcoming)) <https://arxiv.org/abs/1905.07059> (with Carrie Gardner, Abby Waliga, and Sarah Churchman).
 - **Invited Briefings, United States Department of Defense:**
 - *June 2016* – Assistant Secretary of Defense for Homeland Defense and Global Security
 - *January 2016* – Principal Deputy Director, Cost Assessment and Program Evaluation
 - *September 2017* – Commanding General, U.S. Army NETCOM and Deputy Commander, U.S. Army Cyber
- *Chameleon: Effective Honeynet Operation*, Women in Cybersecurity, Mar. 31, 2017 (Tuscon, AZ) (with Carrie Gardner, Sarah Churchman, M. Shannon Bradley, and Adeline Giritharan).
- *Ancient Worries and Modern Fears: Different Roots and Common Effects of U.S. and EU Privacy Regulation*, 49 CONNECTICUT LAW REVIEW 1621 (2017) (with Pierluigi Perri), <http://ssrn.com/abstract=2596382>.
- *Cybersecurity Stovepiping*, 96 NEBRASKA LAW REVIEW 339 (2017), <http://ssrn.com/abstract=2572012>.
 - **Invited Allied Governmental Briefings:** Republic of Korea – National Assembly Legislation Research Institute (July 2015); Republic of Poland – Office of Electronic Administration (Apr. 2015)
- *Data Breach (Regulatory) Effects*, 2015 CARDOZO LAW REVIEW DE NOVO 151, <http://ssrn.com/abstract=2595297>.
- *Reasonable Expectations of Privacy Settings: Contemplating the Stored Communications Act Through the Prism of Social Media*, 13 DUKE LAW & TECHNOLOGY REVIEW 36 (2015) (with Christopher J. Borchert and Fernando Pinguelo) <http://ssrn.com/abstract=2306839>.

- *Surveillance at the Source*, 103 KENTUCKY LAW JOURNAL 405 (2015), <http://ssrn.com/abstract=2512121>.
- *Enlightened Regulatory Capture*, 89 WASHINGTON LAW REVIEW 329 (2014), <http://ssrn.com/abstract=2298205>.
- *The Efficacy of Cybersecurity Regulation*, 30 GEORGIA STATE UNIVERSITY LAW REVIEW 287 (2014), <http://ssrn.com/abstract=2241838>.
 - **Invited U.S. Congressional Testimony:** *Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?*, Hearing Before the House Energy & Commerce Comm., Subcomm. on Commerce, Mfg., & Trade, 113th Cong. (July 18, 2013)
- *Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement*, 103 JOURNAL OF CRIMINAL LAW & CRIMINOLOGY 907 (2013), <http://ssrn.com/abstract=2226176>.
- *When Machines Are Watching: How Warrantless Use of GPS Surveillance Technology Violates the Fourth Amendment Right Against Unreasonable Searches*, 121 YALE LAW JOURNAL ONLINE 177 (2011) (with Priscilla J. Smith, Nabiha Syed and Albert Wong), <http://ssrn.com/abstract=1942559>.
- *Characterizing, Classifying, and Understanding Information Security Laws and Regulations: Considerations for Policymakers and Organizations Protecting Sensitive Information Assets* (May 12, 2011) (Ph.D. dissertation, University of California, Berkeley (on file with the University of California)), <http://www.davidthaw.com/papers/DavidThawDissertationFinal.pdf>.
- *Proposal for a "Down-the-Chain" Notification Requirement in Online Behavioral Advertising Research and Development* (W3C Workshop on Web Tracking and User Privacy Working Paper, Apr. 28, 2011), <http://www.w3.org/2011/track-privacy/papers/ThawGuptaAgrawala.pdf> (with Neha Gupta and Ashok Agrawala).
- *CoPE: Democratic CSCW in Support of e-Learning*, in INTELLIGENT COLLABORATIVE E-LEARNING SYSTEMS AND APPLICATIONS (T. Daradoumis, S. Caballe, J. M. Marques and F. Xhafa eds., 2010) (with Jerome Feldman).
- David Thaw, Jerome Feldman and Joseph Li, *CoPE: Democratic CSCW in Support of e-Learning*, 2008 IEEE COMPUTER SOCIETY: PROCEEDINGS OF THE INTERNATIONAL WORKSHOP ON COLLABORATIVE E-LEARNING SYSTEMS & APPLICATIONS 481 (with Jerome Feldman and Joseph Li).
- *Supporting Communities of Learning Practice by the Effective Embedding of Information and Knowledge into Group Activity*, 2008 COMPUTER SOCIETY: PROCEEDINGS OF THE INTERNATIONAL WORKSHOP ON COLLABORATIVE E-LEARNING SYSTEMS & APPLICATIONS 493. (with Sante Caballé and Jerome Feldman).
- *Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware*, in SPYWARE: AN INSIGHT (Ravi Kumar, ed. 2007) (reprint of earlier conference paper) (with Nathaniel Good, Rachna Dhamija, Jens Grossklags, Steven Aronowitz, Deirdre Mulligan, and Joseph Konstan).
- *Communities of Practice Environment*, in THE INTERNET AND SOCIETY (Morgan, Bebbia and Spector eds., 2006) (with Jerome Feldman and Daniel Lee).
- *Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware* 2005 ASSOCIATION OF COMPUTING MACHINERY: PROCEEDINGS OF THE SYMPOSIUM ON USABLE PRIVACY AND SECURITY 43 (with Nathan Good, Rachna Dhamija, Jens Grossklags, Steven Aronowitz, Deirdre Mulligan, and Joseph Konstan).

- *User Choices and Regret: Understanding Users' Decision Process About Consensually Acquired Spyware*, 2 I/S: A JOURNAL OF LAW & POLICY FOR THE INFORMATION SOCIETY 283 (2006) (with Nathaniel Good, Jens Grossklags, Aaron Perzanowski, Deirdre Mulligan and Joseph Konstan), <http://ssrn.com/abstract=2262437>.

RESEARCH WORK-IN-PROGRESS

Cybersecurity Institutions and Regulatory Frameworks

- *Disambiguating "Cyber"* (arguing for an organized understanding of the often-conflated terms "privacy," "data protection," "cybersecurity," "cybercrime," "cyber warfare," and related terms through the axes of (1) normative versus objective evaluation; and (2) the distinctions among private, public, criminal, and international law) (working paper).

Evaluating and Studying Complex Systems

- *Chameleon Cyber Threat Intelligence Gathering System, Cyber Research Environment Network (CyREN) Laboratory, University of Pittsburgh School of Computing and Information* – cybersecurity research project developing a method and system to collect current and prospective cyber threat intelligence data
 - *Simulation-Based Cyber Data Collection Efficacy* (empirical examination of the ability to attract representative attacks to cyber simulations and apply that data to evaluate cybersecurity recommendations) (under revision) <https://arxiv.org/abs/1905.09336>.
 - *Contextualizing Honeypot Technologies: Measuring Data Collection and Deception Capabilities* (systematic review of existing honeypot/honeynet technologies, evaluating those technologies along multiple axes pertaining their data collection, camouflage, interaction, and deception capabilities, to create a analytic framework for evaluating the empirical validity of data collected from cybersecurity simulations) (working paper).
 - *Election Hacking: Proof-of-Concept Model for Studying Adversary Behavior in Election Meddling* (reporting the results of a preliminary study of foreign-based election hacking and influence operations with a focus on capturing the tactics/techniques/procedures (TTPs) of foreign adversaries, utilizing simulations deployed by the CyREN laboratory during the 2018 U.S. federal election cycle) (working paper).

Emerging Technologies and Other Complex Systems

- *Artificial Intelligence Security and Safety Terminology: Characterizing the AI Assurance Space* (defining the problem space of "Artificial Intelligence Security", disentangling this term which actually refers to three separate, discrete problems with different regulatory goals, characterizing the dangers of conflating those problems and presenting a framework for policy responses to address AI and security) (with Carrie Gardner) (working paper).
- *COVID-19 Vaccine Efficacy and the Evidence on Boosters* (review and analysis of the efficacy of the COVID-19 vaccines in use in the U.S., UK, Israel and Qatar (BNT-162b2, mRNA-1273, Ad26.CoV2.S and ChAdOxS-1) (with Bernard Black) (under revision) <https://ssrn.com/abstract=3987991>.
- *Mask or Respirator Evaluation* (tentative title) (empirical examination of the comparative efficacy at preventing exposure to the SARS-CoV-2 pathogen between FFP2/N95-density filtering facepiece respirators (FFRs) and surgical/procedure masks using a randomized controlled clinical trial among subjects in an urban setting based on serology surveillance) (pending re-evaluation per changing pandemic conditions) (with Bernard Black, Jeffrey Whittle, John Meurer, Vladimir Atanasov, et al.).

- *A General Purpose Blockchain* (proof of the ability to reduce arbitrary objects, including data and operations, to “blocks” which can be verified in a distributed fashion using the fundamental science underlying the blockchain proof-of-concept solution to the double-spend problem and therefore blockchains comprising arbitrary objects can directly compute any computable result, enabling both interoperability and more complex operations both on structured and unstructured data than currently contemplated by extant blockchain and cryptocurrency projects) (working paper, *see also* U.S. Patent Application No. 17/422,753 (July 14, 2021), PCT Publication No. WO/2020/150185 (Jan. 14, 2020) (with Hyung Kyu (Will) Kang).

SELECTED RESEARCH FUNDING AWARDS

- *General Purpose Blockchain*, Obnestic, LLC, 3KBICAS, Co., Ltd. and University of Pittsburgh (Principal Investigator) (multi-source faculty teaching buy-out/funded multi-year research leave) (2019 – present)
- *The Mask or Respirator Evaluation (MORE)* (Collaborator), Advancing a Healthier Wisconsin Endowment, Medical College of Wisconsin (\$100,620) (pending re-evaluation per changing pandemic conditions) (2021)
- *Chameleon Project, CyREN Laboratory*, University of Pittsburgh School of Computing and Information (Principal Investigator)
 - School of Computer and Information, Dean’s Startup Funding (\$10,000) (2015 – 2016)
 - Office of the Senior Vice Chancellor for Research, Directed Research Funding (\$150,000) (2016 – 2018)
- *Security-Assisted Data Science Workforce Development in Pennsylvania*, University of Pittsburgh School of Computing and Information (Senior Personnel), National Science Foundation (\$476,903) (2017 – 2020)
- *Ancient Worries and Modern Fears: Different Roots and Common Effects of U.S. and EU Privacy Regulation*, (Principal Investigator) University of Pittsburgh European Studies Center, Jean Monet EU Center of Excellence Faculty Research Grant (\$2,929.68) (2016)

SELECTED PEER REVIEW, PROFESSIONAL SERVICE, AND EDITORIAL ACTIVITIES

- Reporter, Uniform Law Commission, Study Committee on Cybercrime (2020-2021)
- NSF Reviewer 2022
- Peer Referee, OXFORD UNIVERSITY PRESS
- Peer Referee, CAMBRIDGE UNIVERSITY PRESS
- Peer Referee, *IEEE Security & Privacy*
- Peer Referee, *Journal of Cybersecurity*
- Peer Referee, *Journal of Philosophy, Science, and Law*
- Peer Referee, *Journal of the Association for Information Science and Technology*
- Peer Referee, *Journal of Internet Services and Applications*
- Peer Referee, *Yale Law Journal*
- Peer Referee, Social Sciences and Humanities Research Council of Canada – Law Committee
- Advisory Board Member, *SSRN Cybersecurity, Data Privacy & eDiscovery Law & Policy eJournal*

PATENTS

- *A General Purpose Blockchain*, U.S. Patent Application No. 17/422,753 (July 14, 2021), PCT Publication No. WO/2020/150185 (Jan. 14, 2020), <https://patentscope.wipo.int/search/en/detail.jsf?docId=WO2020150185>.

OTHER PROFESSIONAL EXPERIENCE**Thaw Consulting, LLC**, Flower Mound, TX*Managing Member*, October 2021 – Present

Founder and principal of a strategy consulting firm providing advice and consulting on cybersecurity and emerging technologies and related expert witnesses services.

The Obnestic Project, Dallas, TX and Seoul, KR*Co-founder and Chief Scientist*, December 2019 – Present*Acting General Counsel*, July 2020 – July 2021

Co-founder of a technology start-up developing a distributed computation, data analysis, and digital object management application (“app”) platform based on extending the theory of blockchain to coordinating more complex computational problems. Also temporarily performed the duties of the General Counsel.

Medium Holdings, Seoul, KR and Rochester, NY*Member, Global Technical Advisory Board*, November 2021 – Present

Member of corporate technical advisory board for an international blockchain and digital content company.

ELPIS, the Center for IoT Security, Washington, DC*Founding Advisor*, January 2018 – January 2021

Founding Advisory Board Member of a cybersecurity coordination non-profit organization.

3KBICAS, Co., Ltd. and 3KSoft, Inc., Seoul, KR and Redwood City, CA*Advisor*, April 2018 – December 2019

Member of corporate advisory board for an international blockchain and data integration company.

PAX Datatech (Color Platform), Seoul, KR and Singapore*Advisor*, January 2018 – March 2019

Member of corporate advisory board for an international company developing a blockchain dApp platform.

AlphaTrek, Inc., College Park, MD*Special Counsel*, October 2012 – October 2016

(Non-employee) role functionally providing the services of a general counsel to location-based security services startup.

YellowHat Laboratories, Inc., College Park, MD, Washington, DC and Honolulu, HI*Chief Scientist and Special Counsel*, July 2012 – July 2014*Executive Vice-President and Chief Technology Officer*, July 2011 – June 2012

Part of core management team for a cybersecurity startup. Responsible for overseeing all technical development.

Hogan Lovells US LLP (formerly Hogan & Hartson LLP), Washington, DC*Attorney, Privacy and Information Management Practice*, January 2010 – December 2010

Advised clients on privacy and cybersecurity issues, including comprehensive assessments of organizations’ privacy and data security practices, drafting privacy policies and security plans, and providing privacy/security regulatory compliance advice.

International Computer Science Institute, Berkeley, CA*Graduate Student Researcher*, July 2003 – May 2008

Conducted research to develop a web-based content management and collaboration system for non-technical users.

Dewey & LeBoeuf LLP (formerly LeBoeuf, Lamb, Greene & MacRae LLP), New York, NY*Summer Associate*, Summer 2007

United States District Court for the Southern District of New York, New York, NY
Law Intern to the Honorable Victor Marrero (U.S. District Judge), Summer 2006

Samuelson Law, Technology, and Public Policy Clinic, Berkeley, CA
Legal Intern/Technology Researcher, December 2004 – May 2008

Carvel Corporation, Farmington, CT
Webmaster, December 1998 – May 2004
 Responsible for establishing, managing, and scaling up all aspects of the company's first public Internet presence.

Beacon Corporation, College Park, MD
Director, Beacon Project and Laboratory, December 1998 – June 2001
 One of three founders of a research project to develop a marketable wireless emergency location device for college campuses.
 Developed one of the earliest prototypes of context-aware mobile computing (smartphone technology).

United Technologies Corporation, Farmington, CT/Hartford, CT
Information Technology Intern, Summer 2000, Summer 2001, Summer 2002

SELECTED LEGAL BRIEFS

- *Brief of Amici Curiae Professors of Administrative Law in Support of Plaintiffs-Appellants in Stephen C. v. Bureau of Indian Education*, No. 21-15097 (9th Cir. 2021).
- Julie Cohen, Chris Hoofnagle, William McGeeveran, Paul Ohm, Joel Reidenberg, Neil Richards, and David Thaw, *Information Privacy Scholars' Brief in Spokeo, Inc. v. Robins*, 136 S.Ct. 1540 (Sept. 6, 2015), <http://ssrn.com/abstract=2656482>.
- Priscilla J. Smith, Nabiha Syed, David Thaw and Albert Wong, *Brief of Yale Law School Information Society Project Scholars and Other Experts in the Law of Privacy and Technology in United States v. Jones*, 565 U.S. 400 (2012).
- Priscilla J. Smith, Nabiha Syed, David Thaw and Albert Wong, *Information Society Project at Yale Law School Fellows' Brief in Support of Certiorari to the United States Supreme Court in United States v. Pineda-Moreno*, No. 08-30385 (Dec. 17, 2010).

CONFERENCE, KEYNOTE, AND OTHER INVITED PRESENTATIONS

- *Disambiguating Cybersecurity*, Cybersecurity Law and Policy Scholars Conference, University of Minnesota School of Law (remote), Oct. 1-2, 2021.
- *Data Privacy and Security in Healthcare*, Presentation to the Beazley Institute for Health Law and Policy and the National Security Law Association, Loyola University (Chicago) School of Law, Chicago, IL (remote), Feb. 5, 2021.
- *Security or Privacy: Can You Have Both?*, IEEE Virtual Roundtable (hosted by James Bret Michael, Richard Kuhn, and Jeffrey Voss), 53 IEEE COMPUTER 20-30, Sept. 2020.
- *Bot Contracts*, KCon XV, University of the Pacific McGeorge School of Law, Sacramento, CA, Feb. 22, 2020.
- *From Russia With Love*, Cyber Lecture Series Keynote Address, Faculty of Law and Canadian Institute for Cyber Security, University of New Brunswick, Jan. 23, 2020.

- *Law Enforcement and Privacy in Cyberspace and AI, Quantum Computing, and Global Cybersecurity*, Guest Lectures at the Air Force Judge Advocate General's School's Cyber Law Symposium, Maxwell AFB, AL (Nov. 7, 2019)
- *From Russia With Love*, Guest Lecture on Computer Security, University of Notre Dame Department of Computer Science, Apr. 18, 2019.
- *From Russia With Love*, Lecture Series on Cyber Conflict and Geopolitics (Keynote Address), University of North Carolina School of Media and Journalism, Apr. 2, 2019.
- *From Russia With Love*, Workshop on the Regulation of Artificial Intelligence, University of Surrey, Guildford, United Kingdom, Mar. 21-22, 2019.
- *Balancing Innovation and Consumer Protection*, Michigan Technology Law Review Symposium on Data Privacy and Portability in Financial Technology, Ann Arbor, MI, Feb. 23, 2019.
- *Bot Contracts*, North Carolina Journal of Law and Technology Symposium on Blockchain and the Law, Chapel Hill, NC, Feb. 22, 2019.
- *From Russia With Love*, Faculty Workshop Series, University of North Carolina School of Law, Chapel Hill, NC, Feb. 7, 2019.
- *The U.S. Approach to Consumer Data Security*, Hearings on Competition and Consumer Protection in the 21st Century, invited commentary before the United States Federal Trade Commission, Washington, DC, Dec. 11-12, 2018.
- *Information Mischief Under the Trump Administration*, Symposium on The Trump Administration and Administrative Law, Chicago-Kent School of Law, Chicago, IL, Nov. 29-30, 2018.
- *Transforming a Digital Generation: How the Economic and Legal Implications of Blockchain Will Reshape Society* (Keynote Address), Symposium of Blockchain and Trusted Repositories, University of North Carolina, Chapel Hill, NC, Nov. 5, 2018.
- *Transforming a Digital Generation: How the Economic and Legal Implications of Blockchain Will Reshape Society* (Keynote Address), AI & Blockchain: International Symposium on the 4th Industrial Revolution, Seoul National University, Pangyo, KR, Nov. 1, 2018.
- *Hacking Democracy*, Second Annual Northwestern-Penn-Stanford Junior Faculty Forum for Law and STEM, Northwestern University's Pritzker School of Law, Chicago, IL, Sept. 28-29, 2018.
- *Developments in Cyber Law and Regulations*, Seton Hall University Law School Computer Crime Symposium, Princeton, NJ, June 18, 2018.
- *Managing Electoral Cyber Risk*, Privacy Law Scholars Conference, George Washington University Law School, May 30 – 31, 2018.
- *Defining AI Security: An Exposé of the Ambiguous Terminology and the Problem Space*, The Regulation of AI, University of Surrey, United Kingdom, Mar. 7-8, 2018.
- *Blockchain 3.0 and the Future of Ownership*, Blockchain 3.0 Conference, Seoul, KR, Feb. 8, 2018.

- *The CFAA at 30: Problems and Policies*, Journal of Science & Technology Symposium on Cyberlaw, Boston University School of Law, Feb. 2, 2018.
- *Managing Electoral Cyber Risk*, Penn State Law Junior Faculty Exchange, State College, PA, Nov. 9, 2017.
- *Managing Electoral Cyber Risk*, Faculty Workshop Series, Drexel Kline School of Law, Philadelphia, PA, Nov. 7, 2017.
- *The Internet of Things and Cybersecurity*, Cybersecurity and the Law Conference, Albany Law School, Albany, NY, Oct. 19-20, 2017.
- *Fake Identity, Fake News: The Changing Nature of the Cyber Security Threat*, Blouin Creative Leadership Summit, New York, NY, Sept. 18, 2017.
- *Limitations on Cyber Operations and Issues of Sovereignty in Cyberspace*, Advanced Operational Law Conference, United States Strategic Command, Offutt AFB, NE, Sept. 7-8, 2017.
- *Data Privacy Speaker Series*, University of Arizona School of Law, Apr. 20, 2017.
- *State, Local, and Regional Issues in Cybersecurity*, University of Nebraska College of Law, Mar. 17, 2017.
- *AI and Machine Learning for Cybersecurity and Fraud Detection*, Center on Law and Information Policy Conference on Artificial Intelligence, Machine Learning, and Law, Fordham Law School, Feb. 28, 2017.
- *Notre Dame Conference on Data Security*, Notre Dame University Law School, Feb. 24, 2017.
- *Disambiguating Cyber*, Nebro(hi)oklyn 2016/2017 Workshop for Junior Faculty in Law and Technology, The Ohio State University Moritz College of Law, Feb. 3, 2017.
- *Privacy, Security, and Power: The State of Digital Surveillance*, University of Connecticut School of Law, Hartford, CT, Jan. 27, 2017.
- *Redefining Cybersecurity Policy: An Interdisciplinary Approach to Addressing Systemic Failures*, Graduate School of Public Administration, Seoul National University, Dec. 19, 2016.
- *Redefining Cybersecurity Policy: An Interdisciplinary Approach to Addressing Systemic Failures*, School of Information and Library Sciences, University of North Carolina, Nov. 4, 2016.
- *Roundtable on the Application of International Law to Cyber Conflict* and discussion of Scott Shackelford's *iGovernance: the Future of Multi-Stakeholder Governance in the Wake of the Apple Encryption Saga*, N.C. J. of Int'l Law Symposium on Cyberwarfare and International Law, School of Law, University of North Carolina, Nov. 4, 2016.
- *Transatlantic Perspectives of Privacy and Cybersecurity: A Proposal*, Information Society Project Speaker Series, Yale Law School, Oct. 25, 2016 (with Pierluigi Perri).
- *Interdisciplinary Issues in Information Security*, Guest Lecture in CMSC417 (Computer Networks), Dep't of Computer Science, University of Maryland, College Park, MD, Oct. 14, 2016.

- *Cyber Hygiene: The Importance of Recognizing Social Engineering Attacks*, NATO Allied Command Transformation Cybersecurity Awareness Month, NATO ACT Norfolk, VA, Oct. 12, 2016.
- *Cyber Deterrence, Denying Benefit: Whole of Nation Responses*, USCYBERCOM Legal 2016: Cyber National Security – the Law of Cyberspace Confrontation, United States Cyber Command, U.S. Dep't of Defense, Oct. 3-4, 2016.
- *Leveraged Whack-a-Mole: the Need for Interdisciplinary and Cross-Departmental Approaches to Cyber Defense*, TPRC: 44th Research Conference on Communications, Information, and Internet Policy, George Mason University, Sept. 30-Oct. 1, 2016.
- *Does Cybersecurity Need More Law?*, IEEE Intelligence and Security Informatics 2016, University of Arizona, Sept. 28-30, 2016 (with Derek Bambauer).
- *Cyber Capabilities and the Rules of War*, Blouin Creative Leadership Summit, New York, NY, Sept. 19-20, 2016.
- *Chameleon Cyber Threat Intelligence Gathering System*, Briefing to the Commanding General, U.S. Army Network and Enterprise Technology Command, U.S. Dep't of Defense (hosted on campus in Pittsburgh, PA), Sept. 15, 2016.
- *Redefining Cybersecurity*, CyberWeek 2016, Tel Aviv University/Prime Minister's Office National Cyber Bureau, Tel Aviv, Israel, June 19, 2016.
- *Cyber Threat Intelligence Gathering and the Role of the Department of Defense in Modern Cyber Defense*, Briefing to the Commanding General, U.S. Army 7th Signal Command (Theater), U.S. Dep't of Defense, Norfolk, VA, June 8, 2016.
- *Redefining Cybersecurity*, Privacy Law Scholars Conference, George Washington University Law School, June 3, 2016.
- *Chameleon Cyber Threat Intelligence Gathering System*, Briefing to the Assistant Secretary of Defense for Homeland Defense and Global Security, U.S. Dep't of Defense, Arlington, VA, May 23, 2016.
- *Redefining Cybersecurity*, Midwestern Privacy Law Scholars Conference, Ohio State University Moritz College of Law, May 16, 2016.
- *Virtual Briefing on the US-EU Privacy Shield*, University of Pittsburgh European Studies Center, Apr. 12, 2016.
- *Data Breach (Regulatory) Effects*, The States of Security: Data Security Regulation at the State Level – Standards Setting, Benjamin J. Cardozo School of Law, Yeshiva University, Apr. 1, 2016.
- *Redefining Cybersecurity*, "NeBrooklyn" 2016 Workshop for Junior Faculty in Law and Technology, University of Nebraska College of Law, Mar. 25, 2016.
- *Redefining Cybersecurity*, Lastowka Cyberlaw Colloquim, University of Pittsburgh, Pittsburgh, PA, Feb. 5-6, 2016.
- *Cyburgh: Process/Evolution of Security Program Capability Improvement*, CERT/SEI/Carnegie Mellon University, Pittsburgh, PA, Feb. 1, 2016.

- *Chameleon Cyber Threat Intelligence Gathering System*, Briefing to the Principal Deputy Director, Cost Assessment and Program Evaluation, U.S. Dep't of Defense (hosted on campus in Pittsburgh, PA), Jan. 19, 2016.
- *Internet and Computer Law – Once More Unto the Breach: The Law & Policy of Data Breaches*, Annual Meeting of the American Association of Law Schools, New York, NY, Jan. 9, 2016.
- *Catalyzing Privacy By Design: Lessons from Other Areas – Security and Environmental*, Georgetown University Law Center, Washington, DC, Jan. 7, 2016.
- *Redefining Cybersecurity: Risk Management for Global Issues in Cybersecurity*, Hallym University of Graduate Studies, Seoul, Korea, Dec. 22, 2015.
- *Security, Psychology, and the Smart City*, Exposed: Privacy, Security, and the Smart City, Illinois Institute of Technology Chicago-Kent College of Law, Chicago, IL, Nov. 6, 2015.
- *Ancient Worries and Modern Fears*, Yale Law School Conference on Federalism(s) and Fundamental Rights – Europe and the United States Compared, New Haven, CT, Oct. 29-31, 2015.
- *Redefining Cybersecurity*, Invited Presentation at the University of Nebraska 8th Annual Space, Cyber, and Telecommunications Conference, Washington, DC, Oct. 29-30, 2015.
- *Cybersecurity Stovepiping*, Amsterdam Privacy Conference, Amsterdam, Netherlands, Oct. 23-26, 2015.
- *Cybersecurity Stovepiping*, Carnegie Mellon University School of Computer Science, CyLab Usable Privacy and Security Laboratory Seminar Series, Pittsburgh, PA, Oct. 8, 2015.
- *Cyber Security: Public/Private Cooperation, Legal Reforms, Social Norms, and Critical Infrastructure*, Blouin Creative Leadership Summit, New York, NY, Sept. 21-22, 2015.
- *Cybersecurity and Privacy in the US and the EU*, Global Legal Developments on the 20th Anniversary of the University of Pittsburgh Center for International Legal Education, Pittsburgh, PA, Sept. 11, 2015.
- *Cybersecurity Stovepiping*, Invited Presentation to the Korea Legislation Research Institute, Sejong City, Korea, July 3, 2015.
- *Cybersecurity Stovepiping*, Privacy Law Scholars Conference, University of California, Berkeley, School of Law, June 4-5, 2015.
- *Cybersecurity Stovepiping*, Third Annual Works-in-Progress Roundtable on Law and Computer Science, University of Pennsylvania School of Law, May 12-13, 2015.
- *Cybersecurity Stovepiping*, European Union Workshop on e-Administration, Torun, Poland, Apr. 29, 2015.
- *What if Everything Reveals Everything?*, (discussing Prof. Scott Peppet's upcoming book chapter) Information Law Faculty Workshop, Fordham Law School, Apr. 17, 2015.
- *Cybersecurity Workshop*, NSF/Berkeley Center for Law and Technology Working Group on Cybersecurity Law Reform, University of California, Berkeley, School of Law, Apr. 9-10, 2015.
- *Cyber Security*, Canada-U.S. Law Institute Conference on "The Digital Border," Case Western Reserve University School of Law, Mar. 19-20, 2015.

- *Cybersecurity Stovepiping*, Technology, Innovation, and Intellectual Property Workshop, University of Connecticut School of Law, Mar. 4, 2015.
- *Ancient Worries and Modern Fears*, Computers, Privacy, and Data Protection Conference 2015 (Sponsored by the Information Society Project at Yale Law School), Brussels, Belgium, Jan. 21-23, 2015.
- *Cybersecurity Stovepiping*, "NeBrooklyn" 2014 Workshop for Junior Faculty in Law and Technology, Brooklyn Law School, Dec. 4-5, 2014.
- *Cybersecurity Laws and Regulations in the Standard-Setting Context*, NIST Workshop on Standards Challenges and Cybersecurity: Implications for Distributed Systems and User Privacy, University of Pittsburgh School of Information Sciences, Nov. 20 – 21, 2014.
- *Cybersecurity Laws and Regulations: From Best Practices to Actual Requirements*, University of Pittsburgh School of Law "Lunch & Learn" Speaker Series, University of Pittsburgh, Nov. 13, 2014.
- *Surveillance at the Source*, Midwestern Privacy Law Scholars Conference, Notre Dame Law School, Oct. 23-24, 2014.
- *Surveillance at the Source*, Kentucky Law Journal Symposium on Data Privacy, University of Kentucky College of Law, Oct. 9-10, 2014.
- *Cyber security*, Blouin Creative Leadership Summit, New York, NY, Sept. 24, 2014.
- *Ancient Worries and Modern Fears*, Privacy Law Scholars Conference, George Washington University Law School, June 6, 2014.
- *Military Cyberspace Operations*, Next Generation of NATO Cyber Defense: Second Workshop for Academic Experts, Roundtable Briefing to the NATO Allied Command Transformation Cyber Defence Capability Group, Spain, Mar. 30-Apr. 4, 2014.
- *Regulating Big Data in Urban Governance*, Smart Law for Smarter Cities: Regulation, Technology, and the Future of Cities, Fordham University School of Law, Feb. 27-28, 2014.
- *Engaging Private Expertise in Regulating Information Security*, 30th Annual Information Technology Conference, Jon. M. Huntsman School of Business, Utah State University, Feb. 25, 2014.
- *Military Cyberspace Operations*, Next Generation of NATO Cyber Defense: Workshop for Academic Experts, Roundtable Briefing to the NATO Allied Command Transformation Cyber Defence Capability Group, National Defense University, Washington, DC, Nov. 20, 2013.
- *Military Cyberspace Operations*, Briefing to the Office of the Deputy Assistant Secretary of Defense for Cyberspace Policy Operations, U.S. Dep't of Defense, Arlington, VA, Nov. 7, 2013.
- *The Efficacy of Cybersecurity Regulation: Examining the Impact of Law on Security Practices*, LISA '13: 27th Large Installation System Administration Conference, USENIX: The Advanced Computing Association, Washington, DC, Nov. 7, 2013.

- *Military Cyberspace Operations*, International Roundtable on Internet Governance & Cyber Conflicts: Models, Regulations, & Confidence Building Measures, SUNY Albany/Moscow State University, New York, NY, Oct. 31-Nov. 1, 2013.
- *Domestic Law, Policy, and Regulation: Intellectual Property and Torts – Cybercrime Reform Proposals*, Cyber Threats & Cyber Realities Conference, Roger Williams University Law School, June 17, 2013.
- *Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement*, Privacy Law Scholars Conference, University of California, Berkeley, School of Law, June 6, 2013.
- *The Computer Fraud and Abuse Act: The Statute That Took Over the Internet, And Why You Should Care*, Yale Law School, Apr. 8, 2013.
- *Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement*, Symposium on Cybercrime, Northwestern University Law School, Feb. 1, 2013.
- *The Efficacy of Cybersecurity Regulation*, Cyberscholars Workshop: Remixing Research, Harvard Law School, Dec. 6, 2012.
- *The Efficacy of Cybersecurity Regulation*, Dep't of Computer Science Faculty Colloquium, Worcester Polytechnic Institute, Nov. 30, 2012.
- *Comparing Management-Based Regulation and Prescriptive Legislation: How to Improve Information Security Through Regulation*, Privacy Law Scholars Conference, George Washington University Law School, June 7, 2012.
- *Overview of Cybersecurity Laws, Regulations, and Policies: From "Best Practices" to Actual Requirements*, University of Maryland Cybersecurity Center Annual Symposium, University of Maryland, College Park, May 16, 2012.
- *Comparing Management-Based Regulation and Prescriptive Legislation: How to Improve Information Security Through Regulation*, Cyberscholars Workshop, Columbia University, Mar. 27, 2012.
- *The Relationship Between Regulatory Models and Information Security Practices*, Privacy Law Scholars Conference, George Washington University Law School, June 3, 2010.

COURSES TAUGHT*(by sponsoring College; cross-listed/interdisciplinary courses marked with *)***Law/Public Policy**

- Administrative Law
- Cybersecurity Law*
- Cybersecurity and Privacy Regulation*
- Cybercrime*
- Cybersecurity and the Law (undergraduate/college-in-high school)*
- Seminar Series in Cyberlaw*
- Criminal Law
- Criminal Procedure
- Business Organizations
- Constitutional Law
- Civil Procedure

Computing & Information Science

- Cybersecurity*
- Cybercrime*
- Cybersecurity Research Laboratory (CyREN)
- Exploring Cybersecurity Law*

BAR ADMISSIONS**Connecticut, District of Columbia, New York, Texas, United States Supreme Court**

* * *

Appendix B: Materials Considered

The following list includes all materials considered in the preparation of this Report and Opinion which were either provided to me by counsel or were created or conducted by me in the course of my preparation of this Report and Opinion. Other materials publicly available may have been consulted, and are cited as appropriate in the Report in the context in which they are discussed as indicated in Sections IV and V.

Materials Provided by Counsel:

1. Opening Expert Report of David Martens
2. Deposition of Oren Dor
3. Exhibits 1-25 to the Deposition of Oren Dor
4. Supplemental Declaration of Oren Dor (Case Docket Document 191-15 Filed 10/15/21)
5. Declaration of Professor Woodrow Hartzog
6. Deposition of Sanchit Karve
7. Declaration of Robert Sherwood
8. First Amended Complaint of Facebook, Inc.¹
9. Plaintiff/Counterclaim Defendant Facebook, Inc.'s Supplemental Response to Defendants/Counterclaim Plaintiff's First and Second Interrogatories²
10. Deposition of Yair Regev
11. Exhibits 1-15 to the Deposition of Yair Regev
12. BT0000132
13. BT0000378
14. BT0001485
15. BT0001493
16. BT0001560
17. BT0001889
18. BT0001890
19. BT0001891
20. BT0001892
21. BT0001893
22. BT0001894
23. BT0001895
24. BT0001896
25. BT0001897
26. BT0001898
27. BT0001899

¹ Note: Plaintiff Meta Platforms, Inc. has been substituted for Plaintiff Facebook, Inc. in this matter.

² See supra n. 1.

Meta Platforms v. BrandTotal
Expert Report and Opinion of Dr. David Thaw

No. 3:20-CV-07182-JCS (N.D. Cal.)
Appendix B || Page 2 of 2

28. BT0001900
29. BT0001901
30. BT0001902
31. BT0001903
32. BT0001904
33. BT0001905
34. BT0001906
35. BT0001907
36. BT0001908
37. BT0001909
38. BT0002954
39. BT0002988
40. BT0002989
41. rapid7_events_export6579616822864780327.export[1].csv
42. redis_full[1].json
43. Case Docket Document 191-3 Filed 10/15/21

Materials Created or Procedures Conducted:

(none)

EXHIBIT 10

[Home](#) > Policy & Procedures

Policy & Procedures

Fee Information

There is no registration fee. However, the Judicial Conference of the United States has established a fee for access to information in PACER. All registered users will be charged as follows:

- Use of the PACER system will generate a \$.10 per-page charge.
- Audio files of court hearings retrieved via PACER will generate a \$2.40 per-file charge.

Acknowledgment of Policies and Procedures

I understand that:

- There is a charge for accessing information in PACER. See the Fee Information section above. PACER provides electronic access to case information in U.S. federal courts. By registering for a PACER account, I assume responsibility for all fees incurred through the usage of this account.
- Certain accounts may be designated, under Judicial Conference policy, as exempt from fees. If my account is exempt from the fee, it is my responsibility to use the account only within the scope of the fee exemption.



Listen I must alert the PACER Service Center to any errors in billing within 90 days of the date of the bill.

This

Page The per-page charge applies to the number of pages that results from any search, regardless of the number of pages viewed, printed, or downloaded. Searches that result in no matches incur a charge for one page of data.

- Users who provide a valid credit or debit card at the time of registration will receive immediate access to court records. Users who do not provide a card number during registration will receive an authentication token via U.S. mail in 7-10 business days.
- Usage is billed on a quarterly basis. Pursuant to Judicial Conference policy, no account is billed for usage of less than \$30 in a quarter.
- Statements, which contain a summary of the charges the account has incurred, are sent in January, April, July, and October. Detailed transaction information is available in the [Manage My Account section](#) of the PACER Service Center website.
- All new accounts automatically default to email billing.
- If a credit card or debit card is provided during registration, usage is automatically billed quarterly to that card. These charges will be billed to the card up to 7 days before the due date listed on your quarterly invoice. Electronic statements will be generated and sent via email. Paper statements will not be mailed to accounts with automatic billing.
- If a credit card or debit card number is not provided at the time of registration, quarterly invoices will be emailed to the email address submitted with this registration request. Users must remit payment through the [mail or online via the PACER Service Center website](#).
- PACER bills that are not paid on time are subject to federal debt collection measures. These measures include, but are not limited to, referral to a private collection agency or the U.S. Department of Treasury for collection. Accounts that are referred to a private collection agency will be assessed substantial collection fees in addition to the outstanding debt owed to the PACER Service Center.



Listen to This Page I will provide accurate and complete information in registering for this account. I will promptly inform the PACER Service Center of any changes to that information.

The PACER account being registered is for my use only, unless specifically designated otherwise on the registration form. I am responsible for preventing unauthorized use of the account. If I believe there has been unauthorized use, I must notify the PACER Service Center immediately by emailing.pacer@psc.uscourts.gov or calling (800) 676-6856.

The PACER Service Center and/or a U.S. federal court reserve(s) the right to:

- Suspend service to any account in which the amount due is not paid by the due date.
- Demand immediate payment, outside of the regularly scheduled billing cycles, of an account at any time that the PACER Service Center determines the action is necessary.
- Notify and seek payment from the firm listed on my account registration if my account balance is not paid by the due date.
- Reject an account registration request that the PACER Service Center determines to be related to an existing PACER account with a past-due balance.
- Suspend service to an account if any part of the information provided to the PACER Service Center as part of this account registration process is fraudulent. Information about the account and any accounts determined to be related to it may be turned over to law enforcement authorities.
- Deny accounts to requesters who have delinquent debts to any federal government agency, in accordance with 31 U.S.C. § 3720B(a).
- Suspend or reduce service to, or otherwise restrict access to PACER by, any account that causes an unacceptable level of congestion or a disruption to the operations of the PACER Service Center, a U.S. federal court, or another PACER user.



Listen to This Page Suspend service to an account at any time that the PACER Service Center or a U.S. federal court determines the action is necessary to prevent fraud or to maintain the security of its computer systems and networks.

- Require prepayment as a condition to resume service for any account that has:
 - Had service suspended or restricted for any reason.
 - Had multiple instances of late payments.
 - Been requested to make immediate payment of fees incurred.

Public Access to Court Electronic Records is supported by user fees. Any attempt to collect data from PACER in a manner that avoids billing is strictly prohibited and may result in criminal prosecution or civil action. PACER privileges will be terminated if, in the judgment of judiciary personnel, they are being misused. Misuse includes, but is not limited to, using an automated process to repeatedly access those portions of the PACER application that do not assess a fee (i.e., calendar events report or case header information) for purposes of collecting case information.

An account determined by the PACER Service Center to be related to an account that has been subject to an action outlined above may also be subject to the same action.

Accounts may be determined to be related based on information obtained by the PACER Service Center during registration or other contact with CM/ECF, PACER, or the PACER Service Center.

If these policies and procedures change in a significant way, information regarding the changes will be posted on the PACER Service Center website (www.pacer.uscourts.gov). It is the account holder's responsibility to check these policies and procedures regularly for changes. Continued use of PACER following the posting of changes will mean that the account holder accepts and agrees to the changes.



PACER Administrative Account (PAA) Billing

Many organizations have asked for their employees to have individual PACER accounts, with the capability to consolidate billing at an organizational level. The PAA will allow an organization to receive a single invoice for charges from all accounts under its PAA.

- The firm must establish a PAA to manage all logins at the PACER Service Center website.
- All charges associated with each individual account are accrued to the PAA. The organization will be financially responsible for all associated accounts. If the balance due on the PAA is not paid in full each quarter, PACER service for all accounts linked to the PAA will be suspended. The PAA will be subject to the collection procedures described in these terms.
- For those who use the PAA, the \$30 waiver per quarter will only apply in the event that the firm billing account total for a quarter is less than \$30.
- If there is a past-due balance associated with a PAA, the account administrator cannot link any new individual accounts until the balance has been paid in full.

[About Us](#)[Announcements](#)[Policy & Procedures](#)[Developer Resources](#)[Privacy](#)[Contact Us](#)

This site is maintained by the Administrative Office
of the U.S. Courts on behalf of the federal Judiciary.

[↑ Back to top](#)



The purpose of this site is to provide information
about locating and filing cases in the federal courts.

Page PACER Service Center

(800) 676-6856

pacer@psc.uscourts.gov



EXHIBIT 11

Service Terms and Conditions

The following service terms and conditions (the “**Terms**”) govern (a) your access to, and use of, www.brandtotal.com (together with its sub-domains, content and services, the “**Site**”); and (b) your access to, and use of, the BrandTotal software-as-a-service (“**SaaS**”) platform and related documentation, features, and services, as well as any fixes, updates or upgrades thereto (collectively, the “**Software**”). Therefore, please read these Terms carefully, since they set out the legal rights and obligations between you and **BrandTotal Ltd.** (together with our respective affiliates and subsidiaries, “**BrandTotal**”, “**we**”, “**our**” or “**us**”) with respect to the subject matter hereof. In these Terms, references to the “**Services**” shall include both the Site and the Software.

By clicking the “I ACCEPT” button or by otherwise accessing or using any part of the Service, you acknowledge that you have reviewed, and that you agree to be bound by, these Terms. Furthermore, you represent and warrant that you are at least 18 years old and, if you are entering into these Terms on behalf of your employer or other legal entity, that you have full authority to bind said employer or other legal entity to these Terms. If you do not agree to these Terms, or do not have authority to bind your employer or other legal entity, please do not accept these Terms, nor access or use the Services. You hereby waive any applicable rights to require an original (non-electronic) signature or delivery or retention of non-electronic records, to the extent not prohibited under applicable law.

1. **Description of Services.** The Site is intended for informational purposes only, although it does allow you to contact us and to access the **Software** and a demo version of the Software. We make the Software available to our customers (each, a “**Customer**”) on a SaaS basis through the Site. The Software allows Customers to monitor and identify marketing campaigns and audience analytics in Customer-selected fields.
2. **Modifications.** We reserve the right, at our discretion, to modify these Terms at any time. Such modification(s) will be effective 10 days following posting of the modified Terms on the Site, and your use of any part of the Software thereafter means that you accept such modifications. We therefore encourage you to check the Site regularly to see the most current Terms.
3. **Right to Use the Services.**
 - 3.1. **Site Access.** For such time as these Terms are in effect, we hereby grant you permission to visit and use the Site provided that you comply with these Terms and applicable law.
 - 3.2. **Subscriptions to Software.** Subject to your compliance with these Terms and payment of applicable subscription fees, BrandTotal hereby grants you, and you accept, a non-exclusive, non-transferable, non-sublicensable, and fully revocable right to access and use the Software, during the Subscription Term (as defined below), for your internal purposes only.
4. **Account.** In order to access and use the Software or a demo version of the Software, you are required to become a Customer. In order to become a Customer, you must create an account (“**Account**”). BrandTotal may, at its sole discretion, approve or reject the opening of the Account. You hereby agree: (i) not to allow anyone other than yourself to access or use your Account, not to create an Account for any third party and not to use the account of any third party without their permission; (ii) to provide accurate and complete Account and login information; (iii) to remain solely responsible and liable for the activity that occurs in connection with your Account; (iv) to keep your Account password secure; and (v) to notify BrandTotal immediately of any breach of security or unauthorized use of your Account. If you wish to delete your Account, you may send an email request to BrandTotal at: info@brandtotal.com.
5. **Restrictions.**
 - 5.1. **Restrictions on Use of the Site.** You shall not, and shall not allow any third party to: (i) copy, distribute or modify any part of the Site without our prior written authorization; (ii) use, modify, create derivative works of, transfer (by sale, resale, license, sublicense, download or otherwise), reproduce, distribute, display or disclose Content (as defined below), except as expressly authorized herein; (iii) disrupt servers or networks connected to the Site; (iv) use or launch any automated system (including without limitation, “robots” and “spiders”) to access the Site; and/or (v) circumvent, disable or otherwise interfere with security-related features of the Site or features that prevent or restrict use or copying of any Content or that enforce limitations on use of the Site.
 - 5.2. **Restrictions on Use of the Software.** You shall not, and shall not allow any third party to: (i) copy, distribute, broadcast, rent, lease, lend, use for timesharing or service-bureau services, export, modify, adapt, translate, enhance, customize, or otherwise create derivative works of, the Software or any part thereof; (ii) reverse engineer, decompile, disassemble, or otherwise attempt to derive the source code of, the Software or any part thereof; (iii) remove or distort any proprietary notices, labels or legends on or in the Software (including when you download or print a copy of any Content); (iv) use any automated means to access or use the Software, nor circumvent or disable any security or technological features of the Software; (v) use, send, upload, post, transmit or introduce any device, code, routine or other item (including without limitation bots, viruses, worms, and Trojan horses) that interferes (or attempts to interfere) with the operation or integrity of the Software, nor any content that is unlawful, infringing, defamatory, deceptive,

obscene fraudulent, harassing, pornographic, or abusive; (vi) use the Software to design or develop any competing product or service that competes with the Software; (vii) use the Software for any unlawful or fraudulent purpose, to breach these Terms, or infringe or misappropriate any third party intellectual property, privacy, or publicity right; (viii) take any action that imposes or may impose, as determined in BrandTotal's sole discretion, a disproportionately large load of incoming requests on the Software infrastructure; or (ix) violate or abuse password protections governing access to the Software.

6. Customer Data.

- 6.1. License to Customer Data. While using the Software, you may choose to provide, upload, import, transmit, post, or make accessible (collectively, "**Provide**") to BrandTotal certain data or software (the "**Customer Data**"). You hereby grant BrandTotal a royalty-free, irrevocable, non-exclusive license to use, process, display, copy and store the Customer Data (as defined below) in order: (i) to provide the Software to you; and (ii) to administer and make improvements to the Software as well as carry out related tasks; and (iii) to collect, use and publish Anonymous Information (defined below), and disclose it to its third party service providers, to provide, improve and publicize BrandTotal's Software and services.
- 6.2. Availability of the Customer Data. You hereby agree and acknowledge that: (i) the Software does not operate as an archive or file storage service and BrandTotal does not store all of your Customer Data ; and (ii) you are solely responsible for the backup of your own Customer Data. You may download certain Customer Data that you Provide to BrandTotal at any time during the respective Subscription Term, or as otherwise set forth herein.
- 6.3. Responsibility. You shall remain solely responsible and liable for the Customer Data and you hereby expressly release BrandTotal from any and all liability arising from BrandTotal's use of the Customer Data as permitted herein.

7. **Representation and Warranties.** You hereby represent and warrant that: (i) you own or have obtained the rights to all of the intellectual property rights subsisting in the Customer Data and that you have the right to Provide BrandTotal the license granted herein to use such Customer Data in accordance with these Terms; (ii) the Customer Data does not infringe or violate any patents, copyrights, trademarks or other intellectual property, proprietary or privacy or publicity rights of any third party; and (iii) you agree to comply with all applicable international, national, state, regional and local laws and regulations in accessing and/or using the Software (or any part thereof) and in performing you obligations hereunder, including without limitation laws relating to privacy, data protection, and exports.

8. Intellectual Property; Trademarks.

- 8.1. Site Content and Marks. The (i) content included and/or incorporated in the Services, including without limitation, the text, documents, articles, brochures, descriptions, products, software, graphics, photos, sounds, videos, interactive features, and services (collectively, the "**Content**"); and (ii) the trademarks, service marks and logos contained therein (the "**Marks**"), are the property of BrandTotal and/or its licensors and may be protected by applicable copyright or other intellectual property laws and treaties. The BrandTotal logo, and other marks are Marks of BrandTotal or its affiliates. All other trademarks, service marks, and logos used in the Services are the trademarks, service marks, or logos of their respective owners. We reserve all rights not expressly granted in and to the Content.
- 8.2. Rights to Services. All right, title and interest, and full and exclusive ownership rights, in and to the Services, and any and all parts thereof, and all reproductions, corrections, modifications, enhancements, improvements, upgrades, customizations and derivative works (whether or not permitted under these Terms), and all related patent rights, copyrights, trade secrets, trademarks, service marks, related goodwill, including data related your usage thereof, and BrandTotal's intellectual property, and any rights therein not explicitly granted to you hereunder, are reserved to and shall remain solely and exclusively proprietary to BrandTotal (or its licensors).
- 8.3. Customer Data. The intellectual property and all other rights, title and interest of any nature in and to the Customer Data are and shall remain the exclusive property of you and your licensors. Except as expressly set forth herein, nothing in this Agreement shall be construed as transferring any rights, title or interests in or to Customer Data to BrandTotal or any third party.
- 8.4. Anonymous Information. BrandTotal owns all Anonymous Information collected or obtained by BrandTotal via the Software. "**Anonymous Information**" means information about use of the Software which does not enable identification of an individual, such as aggregated and analytics information about use of the Software.
- 8.5. License to Feedback. If you contact us with feedback data (e.g., questions, comments, suggestions or the like) about the Service (the "**Feedback**"), you hereby grant to BrandTotal a royalty-free, fully-paid, non-exclusive, irrevocable, sublicensable, transferrable, perpetual, and worldwide license to use, reproduce, modify, perform, create derivative works from, distribute, display, and otherwise fully exploit, any such Feedback (or any portion thereof) in any manner and for any purTrademarks. BrandTotal has U.S. and common law trademark rights

pending. Any questions with respect to licensing, use, and/or legal matters with respect to DARK MARKETING brand should be directed to at info@brandtotal.com.

9. Term and Termination.

- 9.1. Site. These Terms shall become effective on the date that you first access to or commence use of the Site, until such time as these Terms are terminated in accordance with Section below.
- 9.2. Subscription Term. Your subscription to the Software shall commence on the earlier of: (i) the date that you commence access to or use of the Software; or (ii) the date that we receive payment of any applicable Service subscription fee, and shall continue for a period of 1 month therefrom (the “**Initial Term**”). Thereafter, subject to your payment of any applicable subscription fees, you subscription to the Software shall automatically renew for successive 1-month subscription periods (each a “**Renewal Term**”, and together with the Initial Term, the “**Subscription Term**”). The Subscription Term shall terminate upon the earlier of: (i) termination of the subscription in accordance with Section 10 below; (ii) or termination of these Terms, in accordance with Section 10 below.

10. Termination.

- 10.1. Termination by BrandTotal. You acknowledge and agree that BrandTotal may at any time, for any reason, and without notice to you: (i) discontinue or modify any aspect of the Service, or any part thereof; (ii) terminate this Agreement, with or without cause; and/or (ii) suspend or terminate your access to the Site and/or your subscription to the Software with or without cause, and BrandTotal shall not be liable to you or any third party for any of the foregoing.
- 10.2. Termination By You. If you object to any term or condition of these Terms, or becomes dissatisfied with the Service in any way, your only recourse and sole remedy is: (a) in the event you have an Account, cancel the Account (“**Account Cancellation**”) and immediately cease using the Software; and (b) in the event you are a Site user, immediately cease using the Site. You may also terminate your subscription to the Software by completing Account Cancellation. You agree, however, that any Account Cancellation or termination of these Terms or you Subscription to the Software in accordance with this Section 10.2, shall not derogate from any payment obligations you may have towards BrandTotal under these Terms.
- 10.3. Suspension. If we believe that you using the Software in a manner that may cause harm to BrandTotal or any third party then we may, without derogating from our right to terminate your access to and use of the Site and/or Software for any breach hereof, suspend your access to and use of the Software until such time as we believe the threat of harm, or actual harm, has passed.

11. Effect of Termination.

- 11.1. General. Upon termination of these Terms and/or your subscription to the Software, you shall immediately discontinue all access and use of the applicable Service (cease using the Software and/or access to the Site, as applicable) and shall promptly, but in any event within three (3) days, permanently delete all copies of the any documentation provided to you in connection with the Software, that are in your possession or control.
- 11.2. Access to Customer Data. Upon termination of these Terms, you will lose all access to any Customer Data that BrandTotal may be storing in order to make available the Software to you. It is your responsibility to download its Customer Data prior to termination of these Terms. Notwithstanding the foregoing, for a period of 30 days from the effective date of termination of these Terms, BrandTotal will provide you, upon your written request, with a reasonable opportunity to download the Customer Data. BrandTotal reserves the right to permanently delete any Customer Data that may be contained in your Account at any time following said 30-day period, and you agree to waive any legal or equitable rights or remedies it may have against BrandTotal with respect to Customer Data that is deleted in connection thereto.
- 11.3. Survival. This Section 11.3, and any section intended to survive termination of these Terms, including without limitation, Sections 6.1 (“*License to Customer Data*”), 7 (“*Representation and Warranties*”), , 8 (“*Intellectual Property; Trademarks*”), 12 (“*Links and Advertisements*”), 13 (“*Disclaimer of Warranties*”), 14 (“*Limitation of Liability*”) and 17 (“*Miscellaneous*”), shall so survive.
12. **Links and Advertisements**. The Services may: (i) contain links to third party websites that are not owned or controlled by BrandTotal; and (ii) display advertisements and other materials not operated or endorsed by BrandTotal. You acknowledge that we assume no responsibility over the items in subparts (i) and (ii) (including the privacy, and other, practices of the third parties that operate or control them) and you agree that we shall not be liable under any circumstances for any loss, damage or injury that results directly or indirectly therefrom. Your use or reliance upon such websites and advertisements is at your sole risk and we encourage you to review the applicable privacy policies and terms of use.
13. **Disclaimer of Warranties**. BRANDTOTAL HEREBY DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED, IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. BRANDTOTAL DOES NOT

WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED, ERROR FREE, OR THAT DEFECTS WILL BE CORRECTED. BRANDTOTAL DOES NOT OFFER A WARRANTY OR MAKE ANY REPRESENTATION REGARDING ANY CONTENT, INFORMATION, OR RESULTS THAT YOU OBTAIN THROUGH THE SERVICES. YOUR USE OF AND RELIANCE UPON THE SERVICES OR CONTENT IS ENTIRELY AT YOUR SOLE DISCRETION AND RISK, AND BRANDTOTAL SHALL HAVE NO RESPONSIBILITY OR LIABILITY WHATSOEVER TO YOU IN CONNECTION WITH ANY OF THE FOREGOING. YOU AGREE THAT WE WILL NOT BE HELD RESPONSIBLE FOR ANY CONSEQUENCES THAT MAY RESULT FROM TECHNICAL PROBLEMS INCLUDING WITHOUT LIMITATION IN CONNECTION WITH THE INTERNET (SUCH AS SLOW CONNECTIONS, TRAFFIC CONGESTION OR OVERLOAD OF OUR OR OTHER SERVERS) OR ANY TELECOMMUNICATIONS OR INTERNET PROVIDERS. Applicable law may not allow the exclusion of certain warranties, so to that extent such exclusions may not apply.

14. **Limitation of Liability.** EXCEPT TO THE EXTENT PROHIBITED BY APPLICABLE LAW, IN NO EVENT SHALL BRANDTOTAL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OF INCOME, PROFITS, GOODWILL, REPUTATION, SPECIAL, INDIRECT, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES THAT ARISE UNDER THESE TERMS OR THAT RESULT FROM THE USE OF, OR THE INABILITY TO USE, THE SERVICE, EVEN IF IT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND EVEN IF DIRECT DAMAGES DO NOT SATISFY A REMEDY. Some jurisdictions do not allow the limitation or exclusion of liability for incidental or consequential damages, so the above limitation may not apply to you. BRANDTOTAL'S TOTAL AGGREGATE LIABILITY FOR ANY AND ALL DAMAGES AND LOSSES UNDER THESE TERMS, OR IN CONNECTION WITH THE USE OF OR INABILITY TO USE THE SERVICE, SHALL NOT UNDER ANY CIRCUMSTANCE EXCEED THE AMOUNT OF FEES ACTUALLY PAID BY YOU TO BRANDTOTAL UNDER THESE TERMS WITHIN THE THREE (3) MONTHS, IF ANY, PRECEDING THE DATE OF BRINGING A CLAIM.
15. **Indemnification.** You agree to defend, indemnify and hold harmless BrandTotal and our affiliates and our respective officers, directors, agents, consultants and employees from any third party claims, damages, liabilities, costs, and expenses (including reasonable attorney's fees) arising from: (i) your use of the Services or any part thereof; and (ii) your breach of these Terms.
16. **Assignment.** These Terms and any rights or obligations hereunder: (i) may not be transferred or assigned by you without the prior written consent of BrandTotal; but (ii) may be transferred or assigned by BrandTotal. Subject to the foregoing conditions, these Terms shall be binding upon and inure to the benefit of each party and its respective assigns. Any prohibited assignment shall be null and void.
17. **Miscellaneous.**
 - 17.1. Independent Contractors. The parties are independent contractors. Nothing in these Terms shall create a partnership, joint venture, agency, or employment relationship between the parties. Neither party may make, or undertake, any commitments or obligations on behalf of the other.
 - 17.2. Governing Law and Jurisdiction. These Terms shall be governed by the laws of the State of Israel, without reference to its conflict of laws rules. The exclusive jurisdiction and venue for all disputes hereunder shall be the courts located in Tel Aviv-Yaffo, and each party hereby irrevocably consents to the jurisdiction of such courts. Application of the United Nations Convention on Contracts for the International Sale of Goods and the Uniform Computer Information Transaction Act are excluded from these Terms. Notwithstanding the foregoing, BrandTotal reserves the right to seek injunctive relief in any court of competent jurisdiction.
 - 17.3. General. These Terms comprise the entire agreement between the parties regarding the subject matter hereof and supersedes and merges all prior understandings, oral and written, between the parties relating to the subject matter of these Terms. If any part of these Terms is held by a court of competent jurisdiction to be illegal or unenforceable, the validity or enforceability of the remainder of these Terms shall not be affected and such provision shall be deemed modified to the minimum extent necessary to make such provision consistent with applicable law and, in its modified form, such provision shall then be enforceable and enforced. No failure or delay in exercising any right hereunder by either party shall operate as a waiver thereof, nor will any partial exercise of any right hereunder preclude further exercise. YOU AGREE THAT ANY CAUSE OF ACTION THAT YOU MAY HAVE ARISING OUT OF OR RELATED TO THE SITE MUST COMMENCE WITHIN ONE (1) YEAR AFTER THE CAUSE OF ACTION ACCRUES. OTHERWISE, SUCH CAUSE OF ACTION IS PERMANENTLY BARRED.

Last updated: June, 2018

EXHIBIT 12

BRANDTOTAL TERMS AND CONDITIONS

PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE USING THE PRODUCTS OR SERVICES OFFERED BY BRANDTOTAL LTD. OR ANY OF ITS AFFILIATES (“**BRANDTOTAL**”). YOU OR THE ENTITY YOU REPRESENT, AS A PROSPECT OR AS A CUSTOMER (WHETHER YOU PURCHASE THE PRODUCTS OR SERVICES DIRECTLY FROM BRANDTOTAL OR THROUGH A CHANNEL PARTNER) (“**YOU**” OR “**YOUR**”) AGREE THAT YOU HAVE READ AND AGREE TO BE BOUND BY AND A PARTY TO THESE TERMS AND CONDITIONS TO THE EXCLUSION OF ALL OTHER TERMS. Capitalized terms not defined herein shall have the meaning set forth on the Sales Order.

Description of the Service and Site. BrandTotal is the owner or licensee of the BrandTotal platform, which enables companies to evaluate their competitors' social advertising and which is made available to you on a software as a service (SaaS) basis (the “**Platform**”) through a web portal on our website, found at www.brandtotal.com.

1. **DEFINITIONS.** The following capitalized terms have the meanings set forth below:

“**Affiliate**” means, with respect to either Party, any person, organization or entity controlling or controlled by such Party. For purposes of this definition only, “control” of another person, organization or entity will mean the possession, directly or indirectly, of the power to direct or cause the direction of the activities, management or policies of such person, organization or entity, whether through the ownership of voting securities, by contract or otherwise. Without limiting the foregoing, “control” will be deemed to exist when a person, organization or entity (i) owns more than fifty percent (50%) of the outstanding voting stock or other ownership interest of the other organization or entity, or (ii) possesses directly the power to elect or appoint more than fifty percent (50%) of the members of the governing body of the other organization or entity.

“**Derivatives**” means any derivatives, analyses, or other intelligence of or about (including without limitation metadata or aggregated data extracted from) Your Data.

“**Feature**” means any module, tool, functionality, or feature of the Services, including without limitation, the hosting, tagging and streaming features.

“**Intellectual Property Rights**” means: (i) patents and patent applications throughout the world, including all reissues, divisions, continuations, continuations-in-part, extensions, renewals, and re-examinations of any of the foregoing; (ii) common law and statutory trade secrets and all other confidential or proprietary or useful information that has independent value, and all know-how, in each case whether or not reduced to a writing or other tangible form; (iii) all copyrights, whether arising under statutory or common law, whether registered or not; (iv) all trademarks, trade names, corporate names, company names, trade styles, service marks, certification marks, collective marks, logos, and other source of business identifiers, whether registered or not; (v) moral rights in those jurisdictions where such rights are recognized; and (vi) all other intellectual property and proprietary rights, and all rights corresponding to the foregoing throughout the world.

“**Permitted User**” means any person that you authorize to access and use the Services.

“**Professional Services**” means installation, deployment, configuration, customization, integration, training, or other professional services.

“**Sales Order**” means BrandTotal's documentation setting the commercial terms which are agreed to in writing by You.

“**Services**” means the services as detailed in the Sales Order.

“**Subscription Scope**” means any Services usage and/or consumption limitations (for example, the use of the Platform solely by Permitted User (as defined below).

“**Subscription Term**” means the Services subscription period specified in the Sales Order.

2. **SUBSCRIPTION**

- 2.1. **General.** Subject to the terms and conditions of this Agreement, to the extent You enters into a paid subscription with BrandTotal, BrandTotal hereby grants You a non-exclusive, non-transferable, non-sublicenseable right to access and use and interact with the Platform, for the number of named users subscribed in the applicable Sales Order, during the Subscription Term, solely for Your internal business purposes. Notwithstanding the foregoing, if You are provided access to the Product solely for purposes of considering the purchase of a subscription to the Product, using the Product through the Free Trial section of BrandTotal’s website, or if a Sales Order specifies that an evaluation subscription is being granted thereunder (“**Evaluation**” or “**POC**”), then in lieu of the foregoing license grant, BrandTotal hereby grants to You a nonexclusive, non-transferable, non-sub-licensable, non-production, revocable, limited right to use the Product, free of charge, for the sole purpose of evaluating whether to purchase a Product subscription, subject to the terms hereof.
- 2.2. **Account Setup.** BrandTotal shall perform the initial Services setup activities, (the “**Initial Setup**”). You shall fully cooperate with BrandTotal in such efforts, and shall provide BrandTotal with all information, access and other resources necessary to achieve the Initial Setup. You warrant that all information submitted during the registration process is, and will thereafter remain, complete and accurate. You shall be responsible and liable for all activities that occur in connection with your use of the Account, including the use by Permitted Users. You will require that all Permitted Users keep user ID and password information strictly confidential and not share such information with any unauthorized person.
- 2.3. **Permitted Users.** Subject to the Subscription Scope, Your use of the Account (to be accessed and/or used solely by Permitted Users). You acknowledges and agrees: (i) to keep, and ensure that Permitted Users keep all Account login details and passwords secure at all times; and (ii) to promptly notify BrandTotal in writing if You become aware of any unauthorized access or use of Your Account or the Platform. You shall ensure that the Permitted Users comply with the terms of this Agreement and shall be solely responsible for any breach of this Agreement by a Permitted User.
- 2.4. **Restrictions.** Except as expressly permitted otherwise under this Agreement, You shall not do (or permit or encourage to be done) any of the following license restrictions (in whole or in part): (a) copy, “frame” or “mirror” the Services; (b) sell, assign, transfer, lease, rent, sublicense, or otherwise distribute or make available the Services to any third party (such as offering it as part of a time-sharing, outsourcing or service bureau environment); (c) modify, alter, adapt, arrange, or translate the Services; (d) decompile, disassemble, decrypt, reverse engineer, extract, or otherwise attempt to discover the source code or non-literal aspects (such as the underlying structure, sequence, organization, file formats, non-public APIs, ideas, or algorithms) of, the Services; (e) remove, alter, or conceal any copyright, trademark, or other proprietary rights notices displayed on or in the Services; (f) circumvent, disable or otherwise interfere with security-related or technical features or protocols of the Services; (h) make a derivative work of the Services, or use it to develop any service or product that is the same as (or substantially similar to) it; (i) store or transmit any robot, malware, Trojan horse, spyware, or similar malicious item intended (or that has the potential) to damage or disrupt the Services; (j) employ any hardware, software, device, or technique to pool connections or reduce the number of Users that directly access or use the Services (sometimes referred to as 'virtualisation', 'multiplexing' or 'pooling') in

order to circumvent the Subscription Scope; (k) forge or manipulate identifiers in order to disguise the origin of any data or content inputted or uploaded to, or transmitted through, the Services by You; or (l) take any action that imposes or may impose (as determined in BrandTotal's reasonable discretion) an unreasonable or disproportionately large load on the servers, network, bandwidth, or other cloud infrastructure which operate or support the Services, or otherwise systematically abuse or disrupt the integrity of such servers, network, bandwidth, or infrastructure.

- 2.5. **Support.** BrandTotal shall provide support and maintenance services in accordance with BrandTotal's Service Level Agreement attached as Schedule A hereto, as may be amended from time to time by BrandTotal in its sole discretion. The support and maintenance services may be performed by BrandTotal and/or BrandTotal's certified third party providers. BrandTotal shall be responsible for such service providers' performance of the support and maintenance services.
- 2.6. **Change in Terms.** In order to improve the services, BrandTotal reserve the right to change the Terms & Conditions stated herein at any time. Upon such change BrandTotal will bring it to Your attention by placing a notice on the BrandTotal website, by sending an email, and/or by some other means. The customer may reject the new terms, however, that means customer may no longer be able to use the Services. If You use the Services in any way after a change to the Terms is effective, that means You agree to all of the changes.

Except for changes by BrandTotal as described here, no other amendment or modification of these Terms will be effective unless in writing and signed by the Parties.

3. **PURCHASES VIA CHANNEL PARTNERS**

If You purchased a subscription to the Services through a BrandTotal-authorized reseller, distributor, or similar channel partner ("**Channel Partner**"), then:

- (a) You are granted a subscription to the Platform by and through the Channel Partner, and not directly by BrandTotal.
- (b) The "Subscription Scope" shall be determined with reference to the ordering document executed between You and the Channel Partner ("**Channel Partner Order Form**"), and BrandTotal shall have no responsibility or liability for any discrepancy between the Subscription Scope under such Channel Partner Order Form on the one hand, and the order issued by You to Channel Partner on the other hand;
- (c) Channel Partner shall be responsible for making any applicable payments to BrandTotal;
- (d) BrandTotal may suspend or terminate Your subscription to the Services if BrandTotal does not receive payment from the Channel Partner;
- (e) Under no circumstances shall BrandTotal be required to provide You with any refund; and
- (f) Neither BrandTotal nor the Services will be bound by, or subject to, any representations, warranties, promises, or commitments made by the Channel Partner.

4. **PAYMENT**

- 4.1. **Subscription Fees.** You shall pay BrandTotal the subscription fees specified in the Sales Order (the "**Subscription Fees**") and whatever other fees or charges are specified in the Sales Order ("**Other Fees**", and together with the Subscription Fees, the "**Fees**"). Unless expressly stated otherwise in the Sales Order: (a) all Fees are stated, and are to be paid, in US Dollars; (b) all payments under this Agreement are non-refundable, and are without any right of set-off or cancellation; (c) all Fees are payable, and shall be invoiced, and shall be paid within thirty (30) days after receipt of invoice (which invoice shall include applicable sales tax as an additional and separate line item); and (d) any amount not paid when due will accrue interest on a daily basis

until paid in full, at the lesser of the rate of one and a half percent (1.5%) per month and the highest amount permitted by applicable law.

- 4.2. **Suspension.** BrandTotal reserves right to suspend provision of the Services: (a) if You are forty-five (45) days or more overdue on a payment; (b) if BrandTotal deems such suspension necessary as a result of Your breach under Section 2.4 (*Restrictions*); (c) if BrandTotal reasonably determines suspension is necessary to avoid material harm to BrandTotal or its other customers, including if the Service's cloud infrastructure is experiencing denial of service attacks or other attacks or disruptions outside of BrandTotal's control, or (d) as required by law or at the request of governmental entities.

4.2.1. In the event that sixty (60) days have passed since the beginning of the suspension, the agreement will be considered as terminated and the terms outlined in section 10.3 will apply.

- 4.3. **Taxes.** Amounts payable under this Agreement are exclusive of all applicable sales, use, consumption, VAT, GST, sales and other taxes, duties or governmental charges, except for taxes based upon BrandTotal's net income. In the event that You are required by any law applicable to it to withhold or deduct taxes for any payment under this Agreement, then the amounts due to BrandTotal shall be increased by the amount necessary so that BrandTotal receives and retains, free from liability for any deduction or withholding, an amount equal to the amount it would have received had You not made any such withholding or deduction. If a purchase order (or purchase order number) is required by You in order for an invoice to be paid, then You shall promptly provide such purchase order (or number) to BrandTotal.

5. **RIGHTS AND TITLE**

- 5.1. **Platform.** The Platform is licensed and not sold to You. All Intellectual Property Rights and all other rights, title and interest of any nature in and to the Platform and/or the Generated Data (as defined below), and any Services provided or made available by BrandTotal hereunder, including all modifications, upgrades, customizations and derivative works (whether or not permitted under this Agreement) thereof, are and shall remain the exclusive property of BrandTotal and its licensors. BrandTotal and its licensors reserve any and all rights not expressly granted in this Agreement.
- 5.2. **Feedback.** If BrandTotal receives any feedback (e.g., questions, comments, suggestions or the like) regarding the Platform and/or the Generated Data and/or the Services (collectively, "**Feedback**"), all rights, including Intellectual Property Rights in such Feedback shall belong exclusively to BrandTotal and that such shall be considered BrandTotal's Confidential Information and You hereby irrevocably and unconditionally transfers and assigns to BrandTotal without consideration, all Intellectual Property Rights in such Feedback and waives any and all moral rights that You may have in respect thereto. It is further understood that use of Feedback, if any, may be made by BrandTotal at its sole discretion, and that BrandTotal in no way shall be obliged to make use of any kind of the Feedback or part thereof.
- 5.3. **Generated Data.** All data, images, analysis, reports and other results generated and/or derived as a result of using the Platform, shall be defined as the "**Generated Data**". As between the You and BrandTotal, the Intellectual Property Rights and all other rights, title and interest of any nature in and to the Generated Data are and shall remain the exclusive property of BrandTotal and its licensors. Except as expressly set forth herein, nothing in this Agreement shall be construed as transferring any rights, title or interests to such Generated Data to You or any third party.
- 5.4. **License to Generated Data.** BrandTotal hereby grants You a limited, non-exclusive, revocable, fully paid (subject to the pool of rights purchased under the Sales Order, royalty-free, non-

transferable, perpetual, worldwide license (and to permit Permitted Users to) access and use the Generated Data and Information for its internal use in connection with research and development and training of algorithms only.

- 5.5. **Anonymous Information.** Any anonymous information, which is derived from the use of the Services (i.e., metadata, aggregated and/or analytics information and/or intelligence relating to the operation, support, and/or Your use, of the Platform) which is not personally identifiable information (“**Analytics Information**”) may be used for providing the Service, for development, and/or for statistical purposes. Such Analytics Information is BrandTotal's exclusive property.

6. **CONFIDENTIALITY.**

Each Party (the “Recipient”) may have access to certain non-public or proprietary information and materials of the other Party (the “Discloser”), whether in tangible or intangible form (“Confidential Information”). Confidential Information shall not include information and material which: (a) at the time of disclosure by Discloser to Recipient hereunder, is in the public domain; (b) after disclosure by Discloser to Recipient hereunder, becomes part of the public domain through no fault of the Recipient; (c) was rightfully in the Recipient's possession at the time of disclosure by the Discloser hereunder, and which is not subject to prior continuing obligations of confidentiality; (d) is rightfully disclosed to the Recipient by a third party having the lawful right to do so; or (e) independently developed by the Recipient without use of, or reliance upon, Confidential Information received from the Discloser. The Recipient shall not disclose or make available the Discloser's Confidential Information to any third party (including without limitation by way of publishing), except to its employees, advisers, agents and investors, subject to substantially similar written confidentiality undertakings). Recipient shall take commercially reasonable measures, at a level at least as protective as those taken to protect its own Confidential Information of like nature (but in no event less than a reasonable level), to protect the Discloser's Confidential Information within its possession or control, from disclosure to a third party. The Recipient shall use the Discloser's Confidential Information solely for the purposes expressly permitted under this Agreement. In the event that Recipient is required to disclose Confidential Information of the Discloser pursuant to any Law, regulation, or governmental or judicial order, the Recipient will (a) promptly notify Discloser in writing of such Law, regulation or order, (b) reasonably cooperate with Discloser in opposing such disclosure, (c) only disclose to the extent required by such law, regulation or order (as the case may be). Upon termination of this Agreement, or otherwise upon written request by the Discloser, the Recipient shall promptly return to Discloser its Confidential Information (or if embodied electronically, permanently erase it), and certify compliance writing. Either party may retain a copy of Confidential Information, for archival purposes only, through any system backup or the like, subject to the continuing obligations under this Section.

Notwithstanding anything in this Agreement to the contrary, the pricing and payment terms under the Sales Order are confidential to BrandTotal, and You shall not disclose such Confidential Information to any third party (except its accountants and lawyers), without BrandTotal's prior express written consent.

Notwithstanding termination of this Agreement in accordance with Section 9, the provisions of this Section 6 shall continue to be in effect for a period of three (3) years thereafter.

7. **DISCLAIMERS.**

- 7.1. YOU ACKNOWLEDGES AND UNDERSTANDS THAT EXCEPT AS EXPRESSLY SET FORTH HEREIN: (I) THE SERVICES ARE PROVIDED ON AN “AS IS” BASIS WITHOUT ANY WARRANTIES WHATSOEVER CONCERNING THE USE OR PERFORMANCE OF THE PROGRAM; AND (II) ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, SYSTEM INTEGRATION, NON-INTERFERENCE, ACCURACY, RELIABILITY AND

QUALITY OF THE PROGRAM ARE HEREBY EXPRESSLY DISCLAIMED TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, AND YOU HEREBY EXPRESSLY WAIVES ALL SUCH WARRANTIES. BRANDTOTAL WILL NOT BE LIABLE OR RESPONSIBLE FOR: (a) ANY TECHNICAL PROBLEMS OF THE INTERNET (INCLUDING WITHOUT LIMITATION SLOW INTERNET CONNECTIONS OR OUTAGES); AND/OR (b) ANY ISSUE THAT IS ATTRIBUTABLE TO YOUR HARDWARE OR PLATFORM OR YOUR INTERNET OR DATA SERVICE PROVIDER. BRANDTOTAL DOES NOT OFFER A WARRANTY OR MAKE ANY REPRESENTATION REGARDING ANY GENERATED DATA AND/OR CONTENT, IMAGES, REPORTS, INFORMATION, OR RESULTS THAT YOU OBTAINS THROUGH USE OF THE PLATFORM, OR THAT THE REPORTS ARE COMPLETE OR ERROR-FREE. YOUR USE OF AND RELIANCE UPON THE PLATFORM AND ANY REPORTS IS ENTIRELY AT YOUR SOLE DISCRETION AND RISK, AND BRANDTOTAL SHALL HAVE NO RESPONSIBILITY OR LIABILITY WHATSOEVER TO YOU IN CONNECTION WITH ANY OF THE FOREGOING.

8. **LIMITATION OF LIABILITY**

- 8.1. IN NO EVENT SHALL EITHER PARTY, ITS AFFILIATES, SUPPLIERS, OR ITS LICENSORS BE LIABLE UNDER, OR OTHERWISE IN CONNECTION WITH, THIS AGREEMENT, FOR: (A) ANY CONSEQUENTIAL, INDIRECT, SPECIAL, INCIDENTAL, OR PUNITIVE DAMAGES; (B) ANY LOSS OF PROFITS, BUSINESS, OPPORTUNITY, REVENUE, CONTRACTS, ANTICIPATED SAVINGS, OR WASTED EXPENDITURE; (C) ANY LOSS OF, OR DAMAGE TO, DATA, INFORMATION SYSTEMS, REPUTATION, OR GOODWILL; AND/OR (D) THE COST OF PROCURING ANY SUBSTITUTE GOODS OR SERVICES.
- 8.2. EXCEPT FOR BREACHES OF CONFIDENTIALITY UNDER SECTIONS 6 [CONFIDENTIALITY] AND 9 [INDEMNIFICATION], THE COMBINED AGGREGATE LIABILITY OF EACH PARTY UNDER, OR OTHERWISE IN CONNECTION WITH, THIS AGREEMENT, INCLUDING THE RELATED DATA PROCESSING AGREEMENT ("DPA"), SHALL NOT EXCEED THE AMOUNT ACTUALLY PAID BY YOU UNDER THIS AGREEMENT IN THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE DATE GIVING RISE TO LIABILITY.
- 8.3. THE FOREGOING EXCLUSIONS AND LIMITATION SHALL APPLY: (A) TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW; (B) EVEN IF A PARTY HAS BEEN ADVISED, OR SHOULD HAVE BEEN AWARE, OF THE POSSIBILITY OF LOSSES, DAMAGES, OR COSTS; (C) EVEN IF ANY REMEDY IN THIS AGREEMENT OR THE RELATED DPA (see Section 10.5) FAILS OF ITS ESSENTIAL PURPOSE; AND (D) REGARDLESS OF THE THEORY OR BASIS OF LIABILITY, AND WHETHER IN CONTRACT, TORT (INCLUDING WITHOUT LIMITATION FOR NEGLIGENCE OR BREACH OF STATUTORY DUTY), MISREPRESENTATION, RESTITUTION, OR OTHERWISE.

9. **INDEMNIFICATION**

- 9.1. **Indemnification by BrandTotal.** BrandTotal shall defend at its expense, indemnify and hold You harmless from and against any and all finally awarded damages, expenses and liabilities incurred by You arising from a third party's claim alleging that the Services infringe any third party intellectual property right; provided that Your use of the Services complies with this Agreement. If the Services become, or in BrandTotal's opinion is likely to become, the subject of an IP Infringement Claim, then BrandTotal may, at its sole discretion: (a) procure for the You the right to continue using the Services; (b) replace or modify the Services to avoid the IP

Infringement Claim; or (c) if options (a) and (b) cannot be accomplished despite BrandTotal's reasonable efforts, then BrandTotal may terminate this Agreement and in such event and provide a refund for any amount pre-paid by You for such returned Services for the remaining unused period of the license subscription. This Indemnity shall not apply to claims arising as a result of:

(i) Your willful misconduct and/or breach of this Agreement (ii) modifications to the Services made by a party other than BrandTotal or its designee; (iii) Your failure to implement Platform updates provided by BrandTotal specifically to avoid infringement; (iv) combination or use of the Services with equipment, devices or Platform not supplied or authorized by BrandTotal. The foregoing constitutes Your sole remedy and BrandTotal's sole liability for any infringement claims.

- 9.2. **Indemnification by You.** You shall defend at its expense, indemnify and hold BrandTotal harmless from and against any and all finally awarded damages, expenses and liabilities incurred by BrandTotal and/or any affiliate thereof in connection with any and all third party claims, demands, or actions arising out of Your use of the Services and/or violation of applicable laws; provided that such claim did not result from BrandTotal's willful misconduct.
- 9.3. **Procedure.** As a condition to the indemnity set forth above, the indemnified party shall provide the indemnifying party prompt notice of any such claim made against it, and grant the indemnifying party sole control of the defense in such claim, and reasonably assist in defending the claim. The indemnified party will not be bound by any settlement that the indemnifying party enters into without the indemnified party's prior written consent, such consent not to be unreasonably withheld.

10. **TERM AND TERMINATION**

- 10.1. **Term.** Unless terminated earlier in accordance herewith, this Agreement shall commence on the date set forth in the applicable Sales Order, and shall continue in full force and effect for the duration of the subscription term (the "**Term**").
- 10.2. **Termination for Breach.** Each Party may terminate this Agreement immediately upon written notice to the other Party if the other Party commits a material breach under this Agreement and, if curable, fails to cure that breach within thirty (30) days after receipt of written notice specifying the material breach (except that for payment defaults, such cure period will be fifteen (15) days).
- 10.3. **Termination for Bankruptcy.** Each Party may terminate this Agreement upon written notice to the other Party upon the occurrence of any of the following events in respect of such other Party: (a) a receiver is appointed for the other Party or its property, which appointment is not dismissed within thirty (30) days; (b) the other Party makes a general assignment for the benefit of its creditors; (c) the other Party commences, or has commenced against it, proceedings under any bankruptcy, insolvency or debtor's relief Law, which proceedings are not dismissed within thirty (30) days; or (d) the other Party is liquidating, dissolving or ceasing normal business operations..
- 10.4. **Effect of Termination; Survival.** Upon termination of this Agreement for any reason: (a) the Subscription shall automatically terminate, (b) You shall cease all access and use of the Services thereunder, and (c) each Party shall (as directed) permanently erase and/or return all Confidential Information of the other Party in Your possession or control. Following termination, all outstanding Fees and other charges that accrued as of termination, which become immediately due and payable, and if necessary BrandTotal shall issue a final invoice. This Section 10, Section 2.4 (Restrictions), 4 (Payment), 5 (Rights and Title), 6 (confidentiality), 7 (Disclaimer), 8 (Limitation of Liability), 9 (Indemnification), and 12 (Miscellaneous) shall survive termination of this Agreement and any Sales Order, as shall any right, obligation or

provision that is expressly stated to so survive or that ought by its nature to survive. Termination shall not affect any rights and obligations accrued as of the effective date of termination.

11. **Third Party Components.** The Services may include what is commonly referred to as 'open source' software. Under some of their respective license terms and conditions, BrandTotal may be required to provide You with notice of the license terms and attribution to the third party, in which case BrandTotal may provide You with such information (whether via the Services, or otherwise). Notwithstanding anything to the contrary herein, use of the open source software will be subject to the license terms and conditions applicable to such open source software, to the extent required by the applicable licensor (which terms and conditions shall not restrict the license rights granted to You hereunder), and to the extent any such license terms and conditions grant You rights that are inconsistent with the limited rights granted to You in this Agreement, then such rights in the applicable open source license shall take precedence over the rights and restrictions granted in this Agreement, but solely with respect to such open source software. BrandTotal will comply with any valid written request submitted by You to BrandTotal for exercising any rights You may have under such license terms and conditions.

12. **MISCELLANEOUS**

- 12.1. **Entire Agreement and Amendments.** This Agreement (and its annexes) represents the entire agreement of the Parties with respect to the subject matter hereof, and supersedes and replaces all prior and contemporaneous oral or written understandings and statements by the Parties with respect to such subject matter. In entering into this Agreement, neither Party is relying on any representation or statement not expressly specified in this Agreement. Without limiting the generality of the foregoing, this Agreement supersedes the following, each of which shall be deemed rejected, void and of no effect: (i) any shrink-wrap, click-wrap, or similar terms and conditions that accompany, or are included within, the Services, even if use of the Services requires an affirmative "acceptance" thereof; and (ii) any terms or conditions (whether printed, hyperlinked, or otherwise) in any purchase order or other standardized business forms, which purport to supersede, modify or supplement this Agreement. This Agreement may only be amended by a written instrument duly signed by each Party. The section and subsection headings used in this Agreement are for convenience only. This Agreement may be executed in counterparts each of which will be considered an original, but all of which together will constitute one and the same instrument.
- 12.2. **Assignment.** This Agreement may not be assigned, in whole or in part, by either Party without the prior express written consent of the other Party; *except, however*, that either Party may, upon written notice, assign this Agreement in whole to: (A) an Affiliate; or (B) a successor in connection with a merger, consolidation, or acquisition of all or substantially all of the assigning Party's assets or business relating to this Agreement. Any prohibited assignment will be null and void. Subject to the provisions of this Section (*Assignment*), this Agreement will bind and benefit each Party and its respective successors and assigns. Furthermore, any BrandTotal obligation hereunder may be performed (in whole or in part), and any BrandTotal right (including invoice and payment rights) or remedy may be exercised (in whole or in part), by an Affiliate of BrandTotal.
- 12.3. **Governing Law.** With respect to any Sales Orders entered into between You and BrandTotal Inc., this Agreement shall be governed by and construed under the laws of the State of New York without reference to conflict of laws rules or principles, and shall be subject to the exclusive jurisdiction of the competent courts of New York County, New York with respect to any dispute and action arising under or in relation to this Agreement. With respect to any Sales Order entered into between You and BrandTotal Ltd., this Agreement shall be governed by and construed under the laws of the State of Israel without reference to conflict of laws rules or principles, and shall be subject to the exclusive jurisdiction of the competent court of Tel Aviv-Jaffa with respect to

any dispute and action arising under or in relation to this Agreement. Notwithstanding anything to the contrary, BrandTotal may seek injunctive or other equitable relief in any jurisdiction in order to protect its intellectual property rights.

- 12.4. **Severability.** If any provision of this Agreement is held by a court of competent jurisdiction to be illegal, invalid or unenforceable, then: (a) the remaining provisions of this Agreement shall remain in full force and effect; and (b) the Parties agree that the court making such determination shall have the power to limit the provision, to delete specific words or phrases, or to replace the provision with a provision that is legal, valid and enforceable and that most closely approximates the original legal intent and economic impact of such provision, and this Agreement shall be enforceable as so modified in respect of such jurisdiction. In the event such court does not exercise the power granted to it as aforesaid, then such provision will be ineffective solely as to such jurisdiction, and will be substituted (in respect of such jurisdiction) with a valid, legal and enforceable provision that most closely approximates the original legal intent and economic impact of such provision.
- 12.5. **Waiver and Remedies.** No failure or delay on the part of either Party in exercising any right or remedy hereunder will operate as a waiver thereof, nor will any single or partial exercise of any such right or remedy preclude any other or further exercise thereof, or the exercise of any other right or remedy. Any waiver granted hereunder must be in writing, duly signed by the waiving Party, and will be valid only in the specific instance in which given. Except as may be expressly provided otherwise in this Agreement, no right or remedy conferred upon or reserved by either Party under this Agreement is intended to be, or will be deemed, exclusive of any other right or remedy under this Agreement, at law, or in equity, but will be cumulative of such other rights and remedies.
- 12.6. **Relationship.** The relationship of the Parties is solely that of independent contractors, neither Party nor its employees are the servants, agents, or employees of the other, and no exclusivities arise out of this Agreement. Nothing in this Agreement shall be construed to create a relationship of employer and employee, principal and agent, joint venture, franchise, fiduciary, partnership, association, or otherwise between the Parties. Except to the extent required by BrandTotal in connection with the provision of the Services and/or the performance of BrandTotal's obligations hereunder, neither Party has any authority to enter into agreements of any kind on behalf of the other Party and neither Party will create or attempt to create any obligation, express or implied, on behalf of the other Party.
- 12.7. **Privacy.** Each Party agrees to comply with all relevant and applicable privacy policies, laws and regulations as they may be in effect from time to time (“**Relevant Privacy Regulations**”). Each Party agrees to post on its respective website its privacy policies, which shall comply with the Relevant Privacy Regulations. BrandTotal's Privacy Policy, as may be in effect from time to time, can be found at https://privacy.brandtotal.com/website_privacy_policy.pdf.
- 12.8. **Force Majeure.** Neither Party shall have any liability for any performance (excluding payment obligations) under this Agreement that is prevented, hindered, or delayed by reason of an event of Force Majeure (defined below). The Party so affected shall be excused from such performance to the extent that, and for so long as, performance is prevented, interrupted, or delayed by the Force Majeure. If and when performance is resumed, all dates specified under this Agreement shall be automatically adjusted to reflect the period of such prevention, interruption, or delay by reason of such Force Majeure. For purposes of this Agreement, an event of “**Force Majeure**” shall be defined as: (a) fire, flood, earthquake, explosion, pandemic or epidemic (or similar regional health crisis), or act of God; (b) strikes, lockouts, picketing, concerted labor action, work stoppages, other labor or industrial disturbances, or shortages of materials or equipment, not the fault of either party; (c) invasion, war (declared or undeclared), terrorism, riot, or civil

commotion; (d) an act of governmental or quasi-governmental authorities (including without limitation lockdowns); (e) failure of the internet or any public telecommunications network, hacker attacks, denial of service attacks, virus or other malicious Platform attacks or infections, shortage of adequate power or transportation facilities; and/or (f) any matter beyond the reasonable control of the affected Party. For the avoidance of doubt, any problems relating to hosting of the Services by a third party is beyond the reasonable control of BrandTotal. For the avoidance of doubt, Force Majeure shall not include (a) financial distress nor the inability of either party to make a profit or avoid a financial loss, (b) changes in market prices or conditions, or (c) a party's financial inability to perform its obligations hereunder.

- 12.9. **Notices.** All notices required or permitted under this Agreement shall be made in writing and shall be sent by any of (i) email; (ii) personal delivery, reputable overnight courier service (e.g., FedEx, UPS, DHL, etc.); (iii) registered; or (iv) certified mail, return receipt requested, addressed to the other party at the address set forth in the Order. The date of such notice shall be deemed to be the day it is delivered, if delivered via email, personally or by courier, or five (5) days after date of dispatch, if mailed.

[Last updated February 23, 2022]

BrandTotal
Service Level Agreement ("SLA")

As part of its commitment to providing high level service to its customers, BrandTotal sets out below the level of service provided.

1. Definitions

Capitalized terms used in this SLA and not otherwise defined shall have the meaning set forth in the BrandTotal Terms and Conditions. The following defined terms shall have the have meaning set forth below:

“Failure” means a reproducible failure under which the Platform or any part thereof, ceases to operate, materially malfunctions or materially fails to perform in accordance with its specifications provided by

“Support” means standard support services as described herein offered by BrandTotal to Customer. Standard Support is subject to call priority levels as set forth below and as may be amended at BrandTotal discretion from time to time

“Response Time” – means the **initial** response time by BrandTotal to support tickets detailed in the table below.

2. Support Services

2.1. **Priority**. When reporting a Failure, Customer must indicate priority according to the definitions set forth below. BrandTotal will use its reasonable commercial efforts to communicate with Customer about the Failure through the contacts below, within the following target response times:

Priority	Failure Description	Initial Response Time (*)	Time to Resolution (**)
1	The BrandTotal Platform is not working or a key functionality of the BrandTotal Platform is not properly working, negatively impacting the functionality or operation of essentially all of the Client’s business.	Up to 2 hours	1 business day
2	The BrandTotal Platform is partially working or a key functionality of the BrandTotal Platform is partially unavailable, negatively impacting the functionality or operation of the majority of the Client's business.	Up to 4 hours	2 business day
3	Other issues directly connected to the BrandTotal Platform which adversely impact the service for Client.	Up to 24hours	5 business day
4	All non-service-impacting issues	Up to 3 days	NA

SLA – Page 2 of 2

* Response Time shall be during normal US Est business hours

** Time to Resolution: The time it takes BrandTotal to present a work-around, a resolution or a plan for resolution in order to solve the reported issue.

For avoidance of doubt, professional services **are not included** within Support Services.

2.2. Contacts. BrandTotal shall respond to service request submissions made only through email support@brandtotal.com

3. Support Fee. Support Fees are included in the annual price as detailed in the Sales Order.

4. Exceptions:

BrandTotal's obligations hereunder are based on and subject to the Client: (i) complying with the terms and conditions of the Agreement, including this SLA; (ii) complying with BrandTotal's instructions, if any, for performing any corrective action; (iii) being available to collaborate and troubleshoot the issue with BrandTotal, including, but not limited to, via a shared screen session; and (v) immediately notifying BrandTotal upon discovering any issue.

[Last updated February 23, 2022]

EXHIBIT 13

1
2
3
4
5
6
7
8 **UNITED STATES DISTRICT COURT**
9 **NORTHERN DISTRICT OF CALIFORNIA**
10 **SAN FRANCISCO DIVISION**
11
12
13

14 FACEBOOK, INC.

15 Plaintiff,

16 v.

17 BRANDTOTAL LTD., et al.,

18 Defendants.
19
20
21
22
23
24
25
26
27
28

Case No. 3:20-CV-07182

DECLARATION OF MIKE CLARK

Clark
Exhibit_5
2/10/2021

1 I, Mike Clark, declare:

2 1. I submit this declaration in support of Facebook's Opposition to Defendants' *Ex*
3 *Parte* Motion for Temporary Restraining Order in the above-captioned matter. I have personal
4 knowledge of the facts set forth herein, and if called to testify as a witness, I could do so
5 competently under oath.

6 2. I am a Director of Product Management at Facebook. In that role, I am personally
7 involved in Facebook and Instagram's (collectively "Facebook") efforts to prevent data scraping on
8 the Facebook and Instagram platforms. My team investigates potential violations of Facebook's
9 terms and policies, and works with Facebook's policy and legal teams to enforce those policies when
10 we determine they have been violated.

11 3. "Scraping" refers to the unauthorized automated extraction of user data. Scraping can
12 be either "logged-in" or "logged-out." Logged-in scraping involves scraping of data that is behind
13 password protection; logged-out scraping involves scraping of data available even without a
14 password. Logged-in scraping can be difficult to identify and distinguish from other activity by the
15 users.

16 4. Facebook restricts access to its website to authorized users who are logged-in for the
17 purpose of expressing themselves, engaging with one another, and forming communities. Facebook
18 restricts third-parties from using its service without authentication or logging-in, in order to protect
19 its service and users. Facebook has approved means for users to share data with third-parties, such
20 as through distinct Application Programming Interfaces ("APIs"). Facebook does permit third-
21 parties, such as authorized developers and businesses, to use certain APIs as an access point to get
22 data into and out of the Facebook platform with user consent. Third-party developers and businesses
23 with apps or managed services for Facebook must also abide by Facebook's Terms and Platform
24 Policies.

25 5. Scraping is a serious concern for technology companies and platforms, including
26 Facebook, for many reasons. For example:

27 a. Tools designed to scrape can often be used for other bad purposes. Most websites that
28 attempt to defend against scraping have limitations in place that would restrict access

1 or the ability to make unauthorized automated requests. Technologies designed to
2 circumvent these restrictions inherently make the sites less secure and can often be
3 used for other harmful acts, like coordinated inauthentic behavior or submitting
4 fraudulent content takedown requests. Scraping evades system limits and makes it
5 more difficult to employ technological solutions and systems that are designed to
6 detect and differentiate normal user behavior from automated activity, including that
7 caused by malware and other hacking tools.

- 8 b. The use of unauthorized automation to extract data from degrades public trust and
9 confidence. Users rightfully expect companies like Facebook to implement access
10 and scraping restrictions.
- 11 c. Scraping has adverse effects on privacy, free expression, and creative endeavors. A
12 user may provide data to a particular platform based on their trust that the platform
13 will maintain control of their data. Scraped data can include personal and private data
14 as well as content, like photographs, protected by copyright. And while users who
15 install scraping extension may in theory have consented to the collection of their
16 personal information, others who may use shared computers—family members,
17 roommates, friends—have not so consented and may not even be aware that their
18 personal information is being scraped. In the case of advertisements and ad creatives,
19 although advertisement on Facebook are considered publicly viewable, the creative
20 content belongs to the user that created and posted the advertisement, not the user that
21 views the advertisement.
- 22 d. Scraping takes away users' control of their data. Facebook has a direct relationship
23 with a user and commits to protecting the users' data from unauthorized users of its
24 website, such as scrapers. Facebook's third-party APIs are the authorized method by
25 which Facebook can confirm that its users have consented to a third-party's collection
26 of their data from Facebook.
- 27 e. Due to their inherent commercial nature, ads often involve licensed copyrighted
28 works. When the content of a user's advertisement is improperly scraped and

1 removed from Facebook, the user who created the advertising content, including the
2 text and image used in the advertisement, has no ability to consent to its collection
3 and removal from Facebook. If the URL for the advertisement is scraped, both users
4 and non-users who have access to the advertisement URL can access and view the
5 advertisement and advertising metrics even if they were not part of the advertisements
6 intended audience. As a result, scraping can disaggregate content from the creator
7 leading to repeated misuse of proprietary material without credit or payment to the
8 creator.

9 f. Evasion of Facebook's anti-scraping terms or measures also undermines the integrity
10 and operation of its network. Unauthorized automated requests for data, in
11 circumvention of system limits, can burden the systems that support the service,
12 causing slow speeds, limiting functionality, and overall consuming computer
13 processing power intended to keep the network running. This also imposes costs on
14 Facebook because of the infrastructure needed to respond to the automated requests.
15 It also degrades the service being provided to real users.

16 g. Scraping can raise security concerns. Once data is scraped it can be used in ways that
17 users would never have expected when the user posted that content or provided that
18 data to a platform. It can put data in the hands of bad actors. For example, databases
19 of scraped personal information can provide bad actors an easy way to target
20 fraudulent communications. This can be true even if the user information is
21 deidentified or aggregated.

22 For at least these reasons, almost all platforms have terms or policies against scraping, and take
23 affirmative steps to enforce those policies, technologically and/or legally.

24 6. Facebook prohibits scraping of user data in their terms and employ a number of
25 technical measures to detect and disrupt scraping. Facebook makes a substantial investment in
26 technological solutions and policy efforts to prevent scrapers from improperly extracting user data
27 through automation. Facebook maintains a variety of systems that monitor and detect suspicious
28 activity on its website and restrict unauthorized automation from both logged-in and logged-out

1 scrapers. For example, Facebook limits the responses to server calls when we detect that behavior
2 may be automated. Facebook also detects and disrupts unauthorized automated requests on its
3 system by monitoring use patterns that are inconsistent with a human user, using challenge-response
4 tests to determine whether a computer user is human or not, and disabling accounts engaged in
5 automated activity.

6 7. Beyond these technical measures, Facebook has, and enforces, its policies against
7 scraping. The Facebook Terms of Service expressly prohibit users to “access or collect data from
8 our Products using automated means (without our prior permission) or attempt[s] to access data that
9 you do not have permission to access.” Likewise, Instagram’s Terms of Use explicitly prohibit all
10 Instagram users from “creating accounts or collecting information in an automated way without our
11 express permission.” Any user of either the Facebook or Instagram Platform must abide by the terms
12 of service that govern the particular platform. I understand that Michael Duffey has submitted a
13 declaration identifying and attaching the relevant Terms of Service.

14 8. Facebook’s anti-scraping policies are part of Facebook’s attempt to strike a careful
15 and thoughtful balance between protecting user data and offering platform access to authorized
16 third-parties. Facebook devotes substantial resources and works constantly to enforce its anti-
17 scraping policies against anyone who engages in unauthorized extraction of user data.

18 9. The Facebook policies against scraping are important to protect user data. Although
19 not every instance of scraping constitutes malicious behavior, I understand that it can be difficult to
20 determine whether scraping is engaged in for benign or malicious purposes. Facebook therefore
21 enforces its anti-scraping policies regardless of who is doing it or how they are using the scraped
22 information. Facebook does not authorize users or developers to deviate from the terms of service.

23 10. Even beyond the security considerations as they relate to its user, Facebook’s right to
24 enforce its policies against scraping is important to protect user privacy more broadly by maintaining
25 the integrity of its platform for the reasons I described above, and to deter third parties from
26 engaging in unauthorized conduct.

27 11. And in addition to all of the considerations described above, processing personal data
28 consistent with user expectations is essential to complying with modern data protection law and

1 regulation. It is therefore in the public interest for companies collecting personal data to properly
2 limit unauthorized extraction and collection of that data through methods that are inconsistent with
3 the purpose and scope of the original disclosure. To do so, companies must be able to guarantee to
4 their users that they will only grant access to data in ways consistent with the user's expectations.
5 Prohibiting companies such as Facebook from implementing technological and legal safeguards for
6 user data is not only against the individual users' interests, it could also subject Facebook to fines or
7 suits in many jurisdictions around the world.

8 12. These concerns are not hypothetical. Facebook entered into a widely-publicized \$5
9 billion settlement with the Federal Trade Commission resulting in a consent decree ordering
10 Facebook to implement certain procedures to further enhance consumer protection and user privacy.
11 A copy of the Federal Trade Commission Order is attached hereto as Exhibit 1. In compliance with
12 the Federal Trade Commission Order, Facebook is required to report scraping covered incidents to
13 the FTC. Based on the investigation done in this case (I understand that Sanchit Karve has
14 submitted a declaration describing the investigation and findings), the browser extensions distributed
15 and used by BrandTotal and Unimania qualify as scraping covered incidents and will be reported to
16 the FTC. Failure to do so would subject Facebook to penalties.

17 13. As a result of the above-mentioned investigation, we observed that Defendants were
18 engaging at least two methods of scraping, which included (i) logged-in scraping by using the users'
19 browser as a proxy, and (ii) misappropriating session tokens and user's session IDs, through their
20 app, and then using them to gain access to Facebook to engage in logged-in scraping of user data.
21 BrandTotal and Unimania's access to the Facebook and Instagram platforms has been revoked for
22 violating Facebook's terms and policies against scraping. Facebook is not improperly enforcing
23 against BrandTotal and Unimania.

24 14. Our enforcement process can give developers an opportunity to work with Facebook
25 to address and remediate violations of our terms and policies. Those who provide fulsome
26 cooperation, and whose violations are of a nature that do not require their outright ban from the
27 platform, can sometimes have their access reinstated. I have personally been involved in multiple
28 enforcement actions in which a developer was able to bring themselves into compliance with

1 Facebook's terms and policies such that Facebook was able to restore access. In this case, I am
2 unaware of a request from BrandTotal and Unimania to access Facebook's platform for the purpose
3 of collecting data through . Instead, I only aware of BrandTotal' and Unimania's collection of data
4 through illegitimate means.

5
6 I declare under penalty of perjury that the foregoing is true and correct. Executed at Oakland,
7 California on the 21 day of October, 2020.

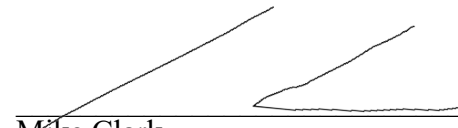
8
9 
10 Mike Clark

EXHIBIT 1

**UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION**

In the Matter of

**FACEBOOK, Inc.,
a corporation.**

Docket No. C-4365

ORDER MODIFYING PRIOR DECISION AND ORDER

The Federal Trade Commission (“Commission”) issued a Decision and Order against Facebook, Inc. (“Facebook”) in Docket C-4365 on July 27, 2012 (“2012 order”).¹ On July 24, 2019, the United States of America, acting upon notification and authorization to the Attorney General by the Commission, filed a complaint (“2019 complaint”) in federal district court alleging that Facebook violated the 2012 order in three ways: (1) by misrepresenting the extent to which users could control the privacy of their data and the steps they needed to take to implement such controls; (2) misrepresenting the information the Company made accessible to third parties; and (3) failing to establish, implement, and maintain a privacy program reasonably designed to address privacy risks. The complaint also alleged that Facebook violated Section 5 of the FTC Act by misrepresenting how it would use telephone numbers that users provided to enable a security feature.

On April 23, 2020, Judge Timothy J. Kelly in the District for the District of Columbia entered a Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief (“Stipulated Order”) resolving the 2019 complaint. In Section II of the Stipulated Order, Facebook consented to: (1) reopening the 2012 proceeding in FTC Docket NO. C-4365; (2) waiving its rights under the show cause procedures set forth in Section 3.72(b) of the Commission’s Rules of Practice, 16 C.F.R. § 3.72(b); and (3) modifying the 2012 Order with the new Decision and Order set forth below.

In view of the foregoing, the Commission has determined that it is in the public interest to reopen the proceeding in Docket No. C-4365 pursuant to Commission Rule 3.72(b), 16 C.F.R. § 3.72(b), and to issue a new order as set forth below. Accordingly,

IT IS ORDERED that this matter be, and it hereby is, reopened; and

IT IS FURTHER ORDERED that, Facebook having consented to modifying the 2012 order as set forth below, the Commission hereby modifies the 2012 order with the attached Decision and Order.

By the Commission, Commissioners Chopra and Slaughter dissenting.

SEAL
ISSUED: April 27, 2020

April J. Tabor
Acting Secretary

¹ *In the Matter of Facebook*, C-4365, 2012 FTC LEXIS 135 (F.T.C. July 27, 2012).

ATTACHMENT A

[182 3109]

**UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION**

In the Matter of

**FACEBOOK, Inc.,
a corporation.**

Docket No. C-4365

DECISION AND ORDER

The Federal Trade Commission (“Commission”) initiated an investigation of certain acts and practices of the Respondent named in the caption. The Commission’s Bureau of Consumer Protection (“BCP”) prepared and furnished to Respondent a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondent with violations of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. §§ 45(a)(1) and (l), 53(b), and 56(a)(1).

The Commission considered the matter and determined that it had reason to believe that Respondent has violated the Decision and Order the Commission previously issued in the matter *In re Facebook, Inc.*, C-4365, 2012 FTC LEXIS 135 (F.T.C. July 27, 2012) and the FTC Act, and that a Complaint should issue stating its charges in that respect. After due consideration, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

FINDINGS

1. This Court has jurisdiction over this matter.
2. The Complaint charges violations of Section 5 of the FTC Act, 15 U.S.C. § 45, and violations of Parts I and IV of an order previously issued by the Commission, 15 U.S.C. § 56(a)(1).
3. Respondent waives any claim that it may have under the Equal Access to Justice Act, 28 U.S.C. § 2412, concerning the prosecution of this action through the date of this Order, and agrees to bear its own costs and attorney fees.
4. Respondent and the Commission waive all rights to appeal or otherwise challenge or contest the validity of this Order.

5. Respondent neither admits nor denies any of the allegations in the Complaint, except as specifically stated in the Decision and Order. Only for purposes of this action, Respondent admits the facts necessary to establish jurisdiction.

DEFINITIONS

For the purpose of this Order, the following definitions apply:

- A. **“Affected Facial Recognition User”** means any User who has a “Tag Suggestions” setting as of the effective date of this Order, and any User who signs up for Respondent’s service after the effective date of this Order and has received the “Tag Suggestions” setting.
- B. **“Clear(ly) and Conspicuous(ly)”** means that a required disclosure is difficult to miss (*i.e.*, easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:
 1. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a video or television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure is made in only one means.
 2. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.
 3. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.
 4. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.
 5. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the representation that requires the disclosure appears.
 6. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.
 7. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.
 8. When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, “ordinary consumers” includes reasonable

members of that group.

C. **“Covered Incident”** means any instance in which Respondent has verified or otherwise confirmed that the Covered Information of 500 or more Users was or was likely to have been accessed, collected, used, or shared by a Covered Third Party in violation of Respondent’s Platform Terms.

D. **“Covered Information”** means information from or about an individual consumer including, but not limited to: (a) a first or last name; (b) geolocation information sufficient to identify a street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging User identifier or a screen name; (d) a mobile or other telephone number; (e) photos and videos; (f) Internet Protocol (“IP”) address, User ID, or other persistent identifier that can be used to recognize a User over time and across different devices, websites or online services; (g) a Social Security number; (h) a driver’s license or other government issued identification number; (i) financial account number; (j) credit or debit information; (k) date of birth; (l) biometric information; (m) any information combined with any of (a) through (l) above; or (n) Nonpublic User Information.

E. **“Covered Third Party”** means any individual or entity that uses or receives Covered Information obtained by or on behalf of Respondent outside of a User-initiated transfer of Covered Information as part of a data portability protocol or standard, other than: (1) a service provider of Respondent that (i) uses the Covered Information for and at the direction of Respondent and no other individual or entity and for no other purpose; and (ii) does not disclose the Covered Information, or any individually identifiable information derived from such Covered Information, except for, and at the direction of, Respondent, for the purpose of providing services requested by a User and for no other purpose; or (2) any entity that uses the Covered Information only as reasonably necessary: (i) to comply with applicable law, regulation, or legal process, or (ii) to enforce Respondent’s terms of use, or (iii) to detect, prevent, or mitigate fraud or security vulnerabilities.

F. **“Facial Recognition Template”** means data, such as a unique combination of numbers or other alphanumeric characters, that is used to predict if the face of a specific User is represented in an image or other visual content.

G. **“Independent Director”** means a member of the Board of Directors other than an executive officer or employee of Respondent or any other individual having a relationship that, in the opinion of the Independent Nominating Committee, would interfere with the exercise of independent judgment in carrying out the responsibilities of such director.

H. **“Independent Privacy Committee”** means a committee of Respondent’s Board of Directors, consisting of Independent Directors, all of whom meet the Privacy and Compliance Baseline Requirements.

I. **“Independent Nominating Committee”** means a committee of Respondent’s Board of Directors, consisting of Independent Directors, the charter of which will encompass, among other things, approving for nomination individuals to the Respondent’s Board of Directors and to the

Independent Privacy Committee.

J. **“Integrity”** means the protection of information from unauthorized destruction, corruption, or falsification.

K. **“Nonpublic User Information”** means any User profile information (*i.e.*, information that a User adds to or is listed on a User’s Facebook profile), or User-generated content (*e.g.*, status updates, photos), that is restricted by one or more Privacy Setting(s).

L. **“Platform Terms”** means Respondent’s written terms, policies, and procedures relating to the privacy, confidentiality, or Integrity of Covered Information that apply to Covered Third Parties.

M. **“Principal Executive Officer”** shall mean Mark Zuckerberg for so long as he serves as Chief Executive Officer or President of Respondent, or such other officer (regardless of title) that is designated in Respondent’s Bylaws or by resolution of the Board of Directors as having the duties of the principal executive officer of Respondent, acting solely in his official capacity on behalf of Respondent; or if Mark Zuckerberg no longer serves in such a position, then such other individual serving as the Chief Executive Officer of Respondent, or such other officer (regardless of title) that is designated in Respondent’s Bylaws or by resolution of the Board of Directors as having the duties of the principal executive officer of Respondent, acting solely in his or her official capacity on behalf of Respondent. In the event that Mark Zuckerberg is not the Principal Executive Officer and such position is jointly held by two or more persons, then each of such persons shall be deemed to be a Principal Executive Officer.

N. **“Privacy and Compliance Baseline Requirements”** shall refer to the requirements that, in the opinion of the Independent Nominating Committee, a member of the Independent Privacy Committee has (1) the ability to understand corporate compliance and accountability programs and to read and understand data protection and privacy policies and procedures, and (2) such other relevant privacy and compliance experience reasonably necessary to exercise his or her duties on the Independent Privacy Committee.

O. **“Privacy Setting”** includes any control or setting provided by Respondent that allows a User to restrict which individuals or entities can access or view Covered Information.

P. **“Representatives”** means Respondent’s officers, agents, servants, employees, attorneys, and those persons in active concert or participation with them who receive actual notice of this Order by personal service or otherwise.

Q. **“Respondent”** means Facebook, Inc. (“Facebook”), its successors and assigns, acting directly, or through any corporation, company, subsidiary, division, affiliate, website, or other device that it directly or indirectly controls. For purposes of Parts VII and VIII, Respondent means Facebook, and its successors and assigns, and WhatsApp Inc., and its successors and assigns.

R. **“User”** means an identified individual from whom Respondent has obtained information

for the purpose of providing access to Respondent's products and services.

I. PROHIBITION AGAINST MISREPRESENTATIONS

IT IS ORDERED that Respondent, including Representatives of Respondent, in connection with any product or service, shall not misrepresent in any manner, expressly or by implication, the extent to which Respondent maintains the privacy or security of Covered Information, including, but not limited to:

- A. Its collection, use, or disclosure of any Covered Information;
- B. The extent to which a consumer can control the privacy of any Covered Information maintained by Respondent and the steps a consumer must take to implement such controls;
- C. The extent to which Respondent makes or has made Covered Information accessible to third parties;
- D. The steps Respondent takes or has taken to verify the privacy or security protections that any third party provides;
- E. The extent to which Respondent makes or has made Covered Information accessible to any third party following deletion or termination of a User's account with Respondent or during such time as a User's account is deactivated or suspended; and
- F. The extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy or security program sponsored by a government or any self-regulatory or standard-setting organization, including but not limited to the EU-U.S. Privacy Shield framework, the Swiss-U.S. Privacy Shield framework, and the APEC Cross-Border Privacy Rules.

II. CHANGES TO SHARING OF NONPUBLIC USER INFORMATION

IT IS FURTHER ORDERED that Respondent and its Representatives, in connection with any product or service, in or affecting commerce, prior to any sharing of a User's Nonpublic User Information by Respondent with any Covered Third Party, which materially exceeds the restrictions imposed by a User's Privacy Setting(s), shall:

- A. Clearly and Conspicuously disclose (such as in a stand-alone disclosure or notice) to the User, separate and apart from any "privacy policy," "data use policy," "statement of rights and responsibilities" page, or other similar document: (1) the categories of Nonpublic User Information that will be disclosed to such Covered Third Parties, (2) the identity or specific categories of such Covered Third Parties, and (3) that such sharing exceeds the restrictions imposed by the Privacy Setting(s) in effect for the User; and
- B. Obtain the User's affirmative express consent.

Nothing in Part II will (1) limit the applicability of Part I of this Order; or (2) require

Respondent to obtain affirmative express consent for sharing of a User's Nonpublic User Information initiated by another User authorized to access such information, provided that such sharing does not materially exceed the restrictions imposed by a User's Privacy Setting(s). Respondent may seek modification of this Part pursuant to 15 U.S.C. § 45(b) and 16 C.F.R. § 2.51(b) to address relevant developments that affect compliance with this Part, including, but not limited to, technological changes and changes in methods of obtaining affirmative express consent.

III. DELETION OF INFORMATION

IT IS FURTHER ORDERED that Respondent and its Representatives, in connection with any product or service, must ensure that Covered Information cannot be accessed by any Covered Third Party from servers under Respondent's control after a reasonable period of time, not to exceed thirty (30) days, from the time that the User has deleted such information or deleted or terminated his or her account, except as required by law or where necessary to protect the Facebook website or its Users from fraud or illegal activity. Nothing in this Part shall be construed to require Respondent to restrict access to any copy of Covered Information that has been posted to Respondent's websites or services by a User other than the User who deleted such information or deleted or terminated such account.

Additionally, Respondent and its Representatives shall further implement procedures designed to ensure that Covered Information entered by the User (such as User-generated content) is deleted from servers under Respondent's control, or is de-identified such that it is no longer associated with the User's account or device, within a reasonable period of time (not to exceed 120 days) from the time that the User has deleted such information, or his or her account, except (1) as required by law; (2) where necessary for the safety and security of Respondent's products, services, and Users, including to prevent fraud or other malicious activity; (3) where stored solely for backup or disaster recovery purposes (subject to a retention period necessary to provide a reliable service); or (4) where technically infeasible given Respondent's existing systems. If a User deletes an individual piece of Covered Information but does not delete his or her account, nothing in this paragraph shall be construed to require deletion or de-identification of metadata (*e.g.*, logs of User activity) that may remain associated with the User's account after the User has deleted such information. Respondent may seek modification of this paragraph pursuant to 15 U.S.C. § 45(b) and 16 C.F.R. § 2.51(b) to address relevant developments that affect compliance with this paragraph, including, but not limited to, technological changes or changes in methods of deleting data.

IV. LIMITATIONS ON THE USE OR SHARING OF TELEPHONE NUMBERS SPECIFICALLY PROVIDED TO ENABLE ACCOUNT SECURITY FEATURES

IT IS FURTHER ORDERED that Respondent and its Representatives, in connection with any product or service, shall not use for the purpose of serving advertisements, or share with any Covered Third Party for such purpose, any telephone number that Respondent has identified through its source tagging system as being obtained from a User prior to the effective date of this Order for the specific purpose of enabling an account security feature designed to protect against unauthorized account access (*i.e.*, two-factor authentication, password recovery, and login alerts). Nothing in Part IV will limit Respondent's ability to use such telephone numbers if obtained separate and apart from a User enabling such account security feature and in a manner consistent with the requirements of this Order.

V. COVERED INFORMATION AND USER PASSWORD SECURITY

IT IS FURTHER ORDERED that Respondent and its Representatives, in connection with any product or service, must implement, and thereafter maintain, a comprehensive information security program that is designed to protect the security of Covered Information. In addition to any security-related measures associated with Respondent's Privacy Program under Part VII of this Order, the information security program must contain safeguards appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the Covered Information. Specifically with respect to the collection, storage, transit, or use of User passwords, such safeguards shall include:

- A. Not requesting or requiring, as part of the User log-in, authentication, or account creation process, User passwords to independent, third-party consumer applications, websites, or other services;
- B. Cryptographically protecting or otherwise securing User passwords when stored and when in transit over the Internet or other similar transmission channel; and
- C. Implementing regular automated scans designed to detect whether any User passwords are stored in plaintext within Respondent's data warehouse, and cryptographically protecting, deleting, or otherwise rendering unreadable any such passwords.

VI. FACIAL RECOGNITION TEMPLATES

IT IS FURTHER ORDERED that Respondent and its Representatives, in connection with any product or service, in or affecting commerce, shall not create any new Facial Recognition Templates, and shall delete any existing Facial Recognition Templates within ninety (90) days from the effective date of this Order, for any Affected Facial Recognition User, unless Respondent Clearly and Conspicuously discloses (such as in a stand-alone disclosure or notice), separate and apart from any “privacy policy,” “data policy,” “statement of rights and responsibilities” page, or other similar documents, how Respondent will use, and to the extent applicable, share, the Facial Recognition Template for such User, and obtains such User’s affirmative express consent.

VII. MANDATED PRIVACY PROGRAM

IT IS FURTHER ORDERED that Respondent, in connection with any product, service, or sharing of Covered Information, shall establish and implement, and thereafter maintain a comprehensive privacy program (“Privacy Program”) that protects the privacy, confidentiality, and Integrity of the Covered Information collected, used, or shared by Respondent. To satisfy this requirement, Respondent must, within 180 days of the effective date of this Order, at a minimum:

- A. Document in writing the content, implementation, and maintenance of the Privacy Program that includes: (1) the documented risk assessment required under Part VII.D. of this Order; (2) the documented safeguards required under Part VII.E. of this Order, including any known alternative procedures that would mitigate the identified risks to the privacy, confidentiality, or Integrity of the Covered Information, but which were not implemented and each reason such procedure(s) were not implemented; (3) a description of the training required under Part VII.G. of this Order; and (4) a description of the procedures adopted for implementing and monitoring the Privacy Program, including procedures used for evaluating and adjusting the Privacy Program as required under Part VII.J. of this Order;
- B. Provide the written program required under Part VII.A. of this Order, and any evaluations thereof or adjustments thereto, to the Principal Executive Officer and to the Independent Privacy Committee created in response to Part X of this Order at least once every twelve (12) months;
- C. Designate a qualified employee or employees to coordinate and be responsible for the Privacy Program (“Designated Compliance Officer(s)”), one of whom will be the Chief Privacy Officer for Product, subject to the reasonable approval of the Independent Privacy Committee, and who may only be removed from such position by Respondent with an affirmative vote of a majority of the Independent Privacy Committee;
- D. Assess and document, at least once every twelve (12) months, internal and external risks in each area of its operation (*e.g.*, employee training and management; developer operations; partnerships with Covered Third Parties; sharing of Covered Information with Covered Third Parties or Facebook-owned affiliates; product research, design, and development; and product marketing and implementation) to the privacy, confidentiality, or Integrity of Covered Information that could result in the unauthorized access, collection, use, destruction, or disclosure of such information. Respondent shall further assess and document internal and external risks as described above as they relate to a Covered Incident, promptly following verification or

confirmation of such an incident, not to exceed thirty (30) days after the incident is verified or otherwise confirmed;

E. Design, implement, maintain, and document safeguards that control for the material internal and external risks identified by Respondent in response to Part VII.D. Each safeguard shall be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized access, collection, use, destruction, or disclosure of the Covered Information.

1. Specifically with respect to any Covered Third Party that obtains or otherwise has access to Covered Information from Respondent for use in an independent, third-party consumer application or website, such safeguards shall include:

- a. Requiring an annual self-certification by each Covered Third Party that certifies: (i) its compliance with each of Respondent's Platform Terms; and (ii) the purpose(s) or use(s) for each type of Covered Information to which it requests or continues to have access, and that each specified purpose or use complies with Respondent's Platform Terms;
- b. Denying or terminating access to any type of Covered Information that the Covered Third Party fails to certify pursuant to Part VII.E.1.a.(ii) above, or, if the Covered Third Party fails to complete the annual self-certification, denying or terminating access to all Covered Information unless the Covered Third Party cures such failure within a reasonable time, not to exceed thirty (30) days;
- c. Monitoring Covered Third Party compliance with Respondent's Platform Terms through measures including, but not limited to, ongoing manual reviews and automated scans, and regular assessments, audits, or other technical and operational testing at least once every twelve (12) months; and
- d. Enforcing against any Covered Third Party violations of Respondent's Platform Terms based solely on the severity, nature, and impact of the violation; the Covered Third Party's malicious conduct or history of violations; and applicable law;

2. Specifically with respect to Respondent's collection, use, or sharing of Covered Information in any new or modified product, service, or practice, such safeguards shall include:

- a. Prior to implementing each new or modified product, service, or practice, (i) conducting a privacy review that assesses the risks to the privacy, confidentiality, and Integrity of the Covered Information, the safeguards in place to control such risks, and the sufficiency of the User notice and, if necessary, consent; and (ii) documenting a description of each reviewed product, service, or practice that was ultimately implemented; any safeguards being implemented to control for the identified risks; and the decision or recommendation made as a result of the

review (*e.g.*, whether the practice was approved, approved contingent upon safeguards or other recommendations being implemented, or rejected);

b. For each new or modified product, service, or practice that presents a material risk to the privacy, confidentiality, or Integrity of the Covered Information (*e.g.*, a completely new product, service, or practice that has not been previously subject to a privacy review; a material change in the sharing of Covered Information with a Facebook-owned affiliate; a modified product, service, or practice that includes a material change in the collection, use, or sharing of Covered Information; a product, service, or practice directed to minors; or a product, service, or practice involving health, financial, biometric, or other similarly sensitive information), producing a written report (“Privacy Review Statement”) that describes:

- (i) The type(s) of Covered Information that will be collected, and how that Covered Information will be used, retained, and shared;
- (ii) The notice provided to Users about, and the mechanism(s), if any, by which Users will consent to, the collection of their Covered Information and the purposes for which such information will be used, retained, or shared by Respondent;
- (iii) Any risks to the privacy, confidentiality, or Integrity of the Covered Information;
- (iv) The existing safeguards that would control for the identified risks to the privacy, confidentiality, and Integrity of the Covered Information and whether any new safeguards would need to be implemented to control for such risks; and
- (v) Any other known safeguards or other procedures that would mitigate the identified risks to the privacy, confidentiality, and Integrity of the Covered Information that were not implemented, such as minimizing the amount or type(s) of Covered Information that is collected, used, and shared; and each reason that those alternates were not implemented;

c. The Designated Compliance Officer(s) shall deliver a quarterly report (“Quarterly Privacy Review Report”) to the Principal Executive Officer and to the Assessor that provides: (i) a summary of the Privacy Review Statements generated during the prior fiscal quarter under Part VII.E.2.b, including a detailed discussion of the material risks to the privacy, confidentiality, and Integrity of the Covered Information that were identified and how such risks were addressed; (ii) an appendix with each Privacy Review Statement generated during the prior fiscal quarter under Part VII.E.2.b; and (iii) an appendix that lists all privacy decisions generated during the prior fiscal quarter under Part VII.E.2.a;

d. The appendices required under Part VII.E.2.c.(ii) and (iii) shall be provided to the Assessor no fewer than twenty-one (21) days in advance of the quarterly meeting of the Independent Privacy Committee as specified in Part X.A.5. A copy of the summary in the Quarterly Privacy Review Report required under VII.E.2.c.(i) shall be provided to Assessor no fewer than fourteen (14) days in advance of the quarterly meeting; and

e. A copy of the Quarterly Privacy Review Report shall also be furnished, upon request, to the Commission;

3. Specifically with respect to Respondent's employees' access to Covered Information maintained in Respondent's data warehouse(s), such safeguards shall include designing, implementing, and maintaining access policies and controls that limit employee access to any table(s) or other comparable data storage units known to contain Covered Information to only those employees with a business need to access such Covered Information;

4. Specifically with respect to Respondent's sharing of Covered Information with any other Facebook-owned affiliate, Respondent shall design, implement, maintain, and document safeguards that control for risks to the privacy, confidentiality, and Integrity of such Covered Information, based on the volume and sensitivity of such Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized access, collection, use, destruction, or disclosure of the Covered Information; and

5. Specifically with respect to facial recognition, such safeguards shall include:

a. Prior to using or sharing any Facial Recognition Template for a User in a manner that materially exceeds the types of uses or sharing disclosed to that User at the time that User's consent was previously obtained,

(i) Clearly and Conspicuously disclosing (such as in a stand-alone disclosure or notice), separate and apart from any "privacy policy," "data policy," "statement of rights and responsibilities" page, or other similar document, how Respondent will use or, to the extent applicable, share, such Facial Recognition Template; and

(ii) Obtaining the User's affirmative express consent;

b. Nothing in this provision shall limit Respondent's ability to use Facial Recognition Templates for fraud prevention or remediation, or protecting the safety, reliability and security of Respondent's platform or Users, so long as Respondent discloses these types of uses in Respondent's privacy policy or similar document;

- F. Assess, monitor, and test, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following the resolution of a Covered Incident, the effectiveness of any safeguards put in place pursuant to Part VII.E. of this Order to address the risks to the privacy, confidentiality, or Integrity of Covered Information, and modify the Privacy Program based on the results;
- G. Establish regular privacy training programs for all employees on at least an annual basis, updated to address any internal or external risks identified by Respondent in Part VII.D. of this Order and safeguards implemented pursuant to Part VII.E. of this Order, that includes training on the requirements of this Order;
- H. Select and retain service providers capable of safeguarding Covered Information they receive from Respondent, and contractually require service providers to implement and maintain safeguards for Covered Information;
- I. Consult with, and seek appropriate guidance from, independent, third-party experts on data protection and privacy in the course of establishing, implementing, maintaining, and updating the Privacy Program; and
- J. Evaluate and adjust the Privacy Program in light of any material changes to Respondent's operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in Part VII.D. of this Order, and any other circumstances that Respondent knows or has reason to believe may have a material impact on the effectiveness of the Privacy Program. Respondent may make this evaluation and adjustment to the Privacy Program at any time, but must, at a minimum, evaluate the Privacy Program at least once every twelve (12) months and modify the Privacy Program as necessary based on the results.

VIII. INDEPENDENT PRIVACY PROGRAM ASSESSMENTS

IT IS FURTHER ORDERED that, in connection with compliance with Part VII of this Order titled Mandated Privacy Program, Respondent must obtain initial and biennial assessments ("Assessments"):

- A. The Assessment must be obtained from one or more qualified, objective, independent third-party professionals ("Assessor(s)"), selected by the Respondent, subject to the reasonable approval of the Independent Privacy Committee and subject to Part VIII.B, who: (1) uses procedures and standards generally accepted in the profession; (2) conducts an independent review of the Mandated Privacy Program; and (3) retains all documents relevant to each Assessment for five (5) years after completion of such Assessment and furnishes such documents to the Commission within ten (10) days of receipt of a written request from a representative of the Commission. No documents may be withheld by the Assessor on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney client privilege, statutory exemption, or any similar claim;
- B. For each Assessment, Respondent must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission ("Associate Director") with the name(s) and affiliation(s) of the person(s) selected to conduct the Assessment, which the

Associate Director shall have the authority to approve;

C. The reporting period for the Assessments must cover: (1) the first 180 days after the Privacy Program has been put in place for the initial Assessment; and (2) each two-year period thereafter for twenty (20) years after issuance of the Order for the biennial Assessments;

D. Each Assessment must: (1) determine whether Respondent has implemented and maintained the Privacy Program required by Part VII.A-J of this Order, titled Mandated Privacy Program; (2) assess the effectiveness of Respondent's implementation and maintenance of each subpart in Part VII of this Order; (3) identify any gaps or weaknesses in the Privacy Program; and (4) identify specific evidence (including, but not limited to, documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is sufficient to justify the Assessor's findings. To the extent that Respondent revises, updates, or adds one or more safeguards required under Part VII.E. of this Order in the middle of an Assessment period, the Assessment shall assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard;

E. Respondent and its Representatives must disclose all material facts to the Assessor(s), and must not misrepresent in any manner, expressly or by implication, any fact material to the Assessor(s)' (1) determination of whether Respondent has implemented and maintained the Mandated Privacy Program required by Part VII of this Order; (2) assessment of the effectiveness of the implementation and maintenance of subparts VII.A-J of this Order; or (3) identification of any gaps or weaknesses to the Mandated Privacy Program;

F. Respondent and its Representatives, whether acting directly or indirectly, must provide or otherwise make available to the Assessor all information and material in their possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege;

G. No finding of any Assessment shall rely primarily on assertions or attestations by Respondent's management. The Assessment shall be signed by the Assessor and shall state that the Assessor conducted an independent review of the Mandated Privacy Program, and did not rely primarily on assertions or attestations by Respondent's management;

H. Each Assessment must be completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Respondent must submit each Assessment to the Commission within ten (10) days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "*In re Facebook, Inc.*, FTC File No. 182-3109." Each Assessment shall be retained by Respondent until this Order is terminated, and shall be provided to the Associate Director within ten (10) days of Request; and

I. The Assessor may only be removed by Respondent from such position, subject to Part VIII.B, with the affirmative vote of a majority of the Independent Privacy Committee.

IX. COVERED INCIDENT REPORTS

IT IS FURTHER ORDERED that Respondent must submit a report within thirty (30) days following Respondent's verification or confirmation of a Covered Incident, and subsequently updated every thirty (30) days until the incident is fully investigated and any remediation efforts are fully implemented, to the Assessor(s) and to the Commission, that includes, to the extent possible:

- A. The date, estimated date, or estimated date range when the Covered Incident occurred;
- B. An overview of the facts relating to the Covered Incident, including the causes of the Covered Incident;
- C. A description of each type of Covered Information that was accessed, collected, used, destroyed, or shared without the User's authorization or consent;
- D. The number of Users whose Covered Information was accessed, collected, used, destroyed, or shared without the User's authorization or consent; and
- E. An overview of the acts, if any, that Respondent has taken to date to remediate the Covered Incident and protect Covered Information from further exposure or access.

Unless otherwise directed by a Commission representative in writing, all reports to the Commission pursuant to this Order must be emailed to Debrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. The subject line must begin, "*In re Facebook, Inc.*, FTC File No. 182-3109."

X. MANDATED INDEPENDENT PRIVACY COMMITTEE AND OTHER GOVERNANCE MATTERS

IT IS FURTHER ORDERED that:

- A. Within one hundred and twenty (120) days after entry of this Order, Respondent shall create the Independent Privacy Committee, including adopting a new committee charter or amending the charter of an existing committee. The adopted or amended charter for such committee shall include the following qualifications, authority, and responsibilities, including:
 - 1. The committee shall hold at least four regularly-scheduled meetings each year;
 - 2. Each member of the committee shall be an Independent Director, and each of the members of the committee shall meet the Privacy and Compliance Baseline Requirements;
 - 3. Each quarter, the Respondent shall cause the committee to receive a briefing from

management regarding (i) the state of the Privacy Program, (ii) Respondent's compliance with the Order, and (iii) material risks to the privacy, confidentiality, and Integrity of the Covered Information that have been discovered since the most recent meeting of the committee or that were raised by management in a prior meeting with the committee and continue to persist;

4. On at least an annual basis, management shall conduct a review for the committee of the Privacy Program and discuss Respondent's assessment of material risks to the privacy, confidentiality, and Integrity of the Covered Information and the steps Respondent has taken or plans to take to monitor or mitigate such risks, including Respondent's procedures and any related policies with respect to risk assessment and risk management;

5. The committee shall meet with the Assessor at least quarterly, and at the conclusion of each biennial Assessment;

a. At each quarterly meeting, the Assessor shall review with management and the committee (i) the Assessor's ongoing assessment of the Privacy Program, and (ii) any material risks to the privacy, confidentiality, and Integrity of the Covered Information that have been identified by the Assessor since the Assessor's most recent meeting with the committee, or that were raised by the Assessor in a prior meeting with the committee and continue to persist;

b. At each quarterly meeting, the committee (together with any other Independent Directors in attendance) shall meet with the Assessor in an executive session without management present to discuss matters involving the Assessment or other privacy-related issues or risks, as appropriate; and

c. At the meeting to review the biennial Assessment with the Assessor, the Assessor and the committee shall review the various elements of the Assessment, as well as (1) any material issues raised by the most recent Assessment or material unresolved issues from prior Assessments, and (2) in an executive session without management present, any problems or difficulties with management. Following the review of the biennial Assessment (at either the same meeting or the following meeting), management shall review with the committee its proposed remediation plans to address any such issues raised in the Assessment; and

6. The committee shall evaluate the independence of the Assessor, and the Assessor shall not be appointed or removed by Respondent, subject to Part VIII.B, without the prior approval of a majority of the committee;

B. Within one hundred and twenty (120) days after entry of this Order, Respondent shall create the Independent Nominating Committee, including adopting a new committee charter or amending the charter of an existing committee to provide that such committee shall have the following authority and responsibilities, including:

1. The committee shall have the sole authority to recommend the appointment of directors, or the nomination of candidates for election, to Respondent's Board of Directors,

such that Respondent's Board of Directors may not approve any such appointment or nomination in the absence of a favorable recommendation from the committee;

2. The committee shall have the sole authority to recommend the appointment of directors to, or the removal of directors from, the Independent Privacy Committee, such that Respondent's Board of Directors may not approve any such appointment or removal in the absence of a favorable recommendation from the committee; and

3. The committee shall determine whether the members of the Independent Privacy Committee qualify as Independent Directors and whether each member of the Independent Privacy Committee meets the Privacy and Compliance Baseline Requirements. The foregoing determinations shall be made prior to, or concurrent with, the formation of the Independent Privacy Committee for the initial members; and prior to, or concurrent with, the appointment of each new director to the Independent Privacy Committee for future members;

C. Within one hundred and eighty (180) days after entry of this Order, Respondent shall adopt and file an amendment to Respondent's Certificate of Incorporation (the "Charter Amendment") in accordance with applicable Delaware law modifying the provisions of Article VI, Section 4 thereof with respect to the removal of directors as set forth in the form attached hereto as Exhibit 1, for the purpose of adding a new Article VI, Section 4(b) (hereafter "Supplemental Removal Provision"). Respondent shall not further alter or amend the Supplemental Removal Provision of Respondent's Certificate of Incorporation for the term of the Order. Notwithstanding the foregoing, in the event that, prior to the effectiveness of the Charter Amendment, any person commences any legal or administrative proceeding or action (an "Action"), or any governmental or regulatory entity or body, or any court, tribunal, or judicial body, in each case whether federal, state, or local, issues or grants any order, judgment, decision, decree, injunction, or ruling that has the effect of delaying, restraining, enjoining, prohibiting, or otherwise preventing the approval, filing, or effectiveness of the Charter Amendment (individually or collectively, a "Restraint") within 180 days after entry of this Order, that time period shall be extended and Respondent shall be deemed to be in compliance with the Order so long as: (a) Respondent diligently pursues in good faith the favorable resolution of such Action, and (b) Respondent adopts and files the Charter Amendment in accordance with applicable Delaware law as promptly as reasonably practicable following the resolution of the Action and at such time as such Restraint (if any) is withdrawn, vacated, or terminated; and

D. Nothing in this Order shall be construed to expand, modify, or alter the fiduciary duties of the members of the Respondent's Board of Directors or any committee thereof.

XI. CERTIFICATIONS

IT IS FURTHER ORDERED that Respondent shall:

A. Within forty-five (45) days after the end of each full fiscal quarter (but in no event later than the first meeting of the Independent Privacy Committee with respect to such fiscal quarter (as provided in Part X.A)) following the anniversary of the effective date of this Order, provide the Commission with its certification, signed by the Principal Executive Officer and the Designated

Compliance Officer(s) on behalf of Respondent, that, with respect to such fiscal quarter: (1) Respondent has established, implemented, and maintained a Privacy Program that complies in all material respects with the requirements of Part VII of this Order; and (2) Respondent is not aware of any material noncompliance with Part VII that has not been corrected or disclosed to the Commission. In making this certification on behalf of Respondent, the Principal Executive Officer shall rely, and be entitled to rely, solely on the following: (a) his or her personal knowledge; (b) sub-certifications regarding compliance with Part VII, provided by knowledgeable personnel charged with implementing the Privacy Program; and (c) the Principal Executive Officer's review of the summaries in the Quarterly Privacy Review Report required under Part VII.E.2.c.(i) for such fiscal quarter, as well as any material issues raised in Covered Incident Reports required under Part IX for such fiscal quarter. The Designated Compliance Officer(s) shall rely, and be entitled to rely, solely on the following: (a) his or her personal knowledge; (b) sub-certifications regarding compliance with Part VII, provided by knowledgeable personnel charged with implementing the Privacy Program; (c) material issues identified in the Quarterly Privacy Review Report required under Part VII.E.2.c.; and (d) material issues raised in the Covered Incident Reports required under Part IX for such fiscal quarter; and

B. Within forty-five (45) days after the end of the first full fiscal quarter (but in no event later than the first meeting of the Independent Privacy Committee with respect to such fiscal quarter (as provided in Part X.A.)) following the anniversary of the effective date of this Order and every year thereafter, provide the Commission with its certification, signed by the Principal Executive Officer and the Designated Compliance Officer(s) on behalf of Respondent, that: (1) Respondent has established, implemented, and maintained the requirements of this Order in all material respects; and (2) Respondent is not aware of any material noncompliance with this Order that has not been corrected or disclosed to the Commission. In making this certification on behalf of Respondent, the Principal Executive Officer shall rely, and be entitled to rely, solely on the following: (a) his or her personal knowledge; (b) sub-certifications regarding compliance with Part VII of this Order, provided by knowledgeable personnel charged with implementing the Privacy Program; and (c) the Principal Executive Officer's review of the written program required under Part VII.A. of this Order and the summaries in the Quarterly Privacy Review Reports required under Part VII.E.2.c.(i) for the preceding year, as well as any material issues raised in Covered Incident Reports required under Part IX for the preceding year. The Designated Compliance Officer(s) shall rely, and be entitled to rely, solely on the following: (a) his or her personal knowledge; (b) sub-certifications regarding compliance with Part VII, provided by knowledgeable personnel charged with implementing the Privacy Program; (c) material issues identified in the Quarterly Privacy Review Reports required under Part VII.E.2.c. for the preceding year; and (d) material issues raised in the Covered Incident Reports required under Part IX for the preceding year.

Unless otherwise directed by a Commission representative in writing, Respondent shall submit all certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "*In re Facebook, Inc.*, FTC File No. 182-3109."

XII. ORDER ACKNOWLEDGMENTS

IT IS FURTHER ORDERED that Respondent obtain acknowledgments of receipt of this Order:

- A. Respondent, within seven (7) days of entry of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury;
- B. For five (5) years after entry of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities for conduct related to the subject matter of the Order and all agents and representatives who participate in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in the Part titled Compliance Reporting. Delivery must occur within seven (7) days of entry of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities; and
- C. From each individual or entity to which Respondent delivered a copy of this Order, Respondent must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order.

XIII. COMPLIANCE REPORTING

IT IS FURTHER ORDERED that Respondent make timely submissions to the Commission:

- A. One hundred eighty (180) days after entry of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, which: (1) identifies the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission may use to communicate with Respondent; (2) identifies all of Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (3) describes the activities of each business; (4) describes in detail whether and how Respondent is in compliance with each Part of this Order; and (5) provides a copy of each Order Acknowledgment obtained pursuant to this Order, unless previously submitted to the Commission;
- B. For twenty (20) years after entry of this Order, Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in the following: (1) any designated point of contact; (2) Respondent's corporate structure; or (3) the structure of any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order;
- C. Respondent must submit to the Commission notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Respondent within fourteen (14) days of its filing;

D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: “I declare under penalty of perjury under the laws of the United States of America that, to the best of my knowledge and reasonable belief, the foregoing is true and correct. Executed on: _____” and supplying the date, signatory’s full name, title (if applicable), and signature; and

E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: “*In re Facebook, Inc.*, FTC File No. 182-3109.”

XIV. RECORDKEEPING

IT IS FURTHER ORDERED that Respondent must create certain records for twenty (20) years after entry of the Order, and retain each such record for five (5) years. Specifically, Respondent must create and retain the following records:

A. All widely-disseminated statements by Respondent or its Representatives that describe the extent to which Respondent maintains and protects the privacy, security, and confidentiality of any Covered Information, including, but not limited to, any statement related to a change in any website or service controlled by Respondent that relates to the privacy of such information, along with all materials relied upon in making such statements, and a copy of each materially different Privacy Setting made available to Users (including screenshots/screencasts of Privacy Settings and the User interfaces, consent flows, and paths a User must take to reach such settings);

B. Records sufficient to identify the types of Covered Information that Respondent provides or makes available to any Covered Third Party that is subject to the requirements of Part VII.E.1., including records identifying: (1) the specific data fields to which access was granted; (2) the means by which the information was provided or made available; (3) the identity of the Covered Third Party to which access was granted; (4) the self-certifications provided by the Covered Third Party (as described in Part VII.E.1); and (5) the date(s) when access was provided;

C. All consumer complaints directed at Respondent or forwarded to Respondent by a Covered Third Party that relate to the conduct prohibited by this Order and any responses to such complaints;

D. Any documents, prepared by or on behalf of Respondent, that contradict, qualify, or call into question Respondent’s compliance with this Order;

E. Each materially different document relating to Respondent’s attempt to obtain the consent of Users referred to in Part II titled Changes To Sharing Of Covered Information, along with documents and information sufficient to show each User’s consent; and documents sufficient to demonstrate, on an aggregate basis, the number of Users for whom each such Privacy Setting was in effect at any time Respondent has attempted to obtain and/or been required to obtain such consent;

F. All materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, for the compliance period covered by such Assessment; and

G. All records necessary to demonstrate full compliance with each Part of this Order, including all submissions to the Commission.

XV. COMPLIANCE MONITORING

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

A. Within fourteen (14) days of receipt of a written request from a representative of the Commission, Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury; appear for depositions; and produce documents for inspection and copying. The Commission is also authorized to obtain discovery, without further leave of court, using any of the procedures prescribed by Federal Rules of Civil Procedure 29, 30 (including telephonic depositions), 31, 33, 34, 36, 45, and 69;

B. For matters concerning this Order, the Commission is authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview any employee or other person affiliated with Respondent who has agreed to such an interview. The person interviewed may have counsel present; and

C. The Commission may use all other lawful means, including posing, through its representatives, as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XVI. ORDER EFFECTIVE DATES

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate 20 years from the date of its issuance, or 20 years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

A. Any Part in this Order that terminates in less than 20 years;

B. This Order's application to any Respondent that is not named as a defendant in such complaint; and

C. This Order if such complaint is filed after the Order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that the Respondent did not violate any Part of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Part as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

April Tabor
Acting Secretary

SEAL:
ISSUED:

ARTICLE VI: MATTERS RELATING TO THE BOARD OF DIRECTORS

4. Term and Removal.

(a) Each director shall hold office until such director's successor is elected and qualified, or until such director's earlier death, resignation or removal. Any director may resign at any time upon notice to the corporation given in writing or by any electronic transmission permitted in the corporation's Bylaws or in accordance with applicable law. No decrease in the number of directors constituting the Whole Board shall shorten the term of any incumbent director.

(b) Notwithstanding anything in this Section 4 of this Article VI to the contrary, subject to the rights of the holders of any series of Preferred Stock with respect to directors elected thereby, from and after the effectiveness of the Classified Board, no director may be removed except for cause and only by the affirmative vote of the holders of at least a majority of the voting power of the then-outstanding shares of capital stock of the corporation then entitled to vote at an election of directors voting together as a single class.

(c) For so long as the [Federal Trade Commission Decision & Order] (the "**Order**") remains in effect, (i) no director serving on the Independent Privacy Committee, as that term is defined in the Order (any such director, a "**Privacy Committee Delegate**"), shall be removed solely for reasons related to actions taken in good faith in furtherance of such Privacy Committee Delegate's duties as a member of the Independent Privacy Committee as set forth in the Order (a "**Privacy Reason**"), except by the affirmative vote of the holders of at least two-thirds of the voting power of the then-outstanding shares of the capital stock of the corporation entitled to vote generally in the election of directors, voting together as a single class, and (ii) no Privacy Committee Delegate shall be removed for reasons other than a Privacy Reason with the intent to circumvent the requirements of clause (i) above, except by the affirmative vote of the holders of at least two-thirds of the voting power of the then-outstanding shares of the capital stock of the corporation entitled to vote generally in the election of directors, voting together as a single class.

EXHIBIT 14

REDACTED VERSION OF
EXHIBIT FILED UNDER
SEAL

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

META PLATFORMS, INC., a)
Delaware corporation)
) CASE NO.
Plaintiff/Counterclaim) 3:20-CV-07182-JCS
Defendant)
)
VS.)
)
BRANDTOTAL, LTD., an)
Israel corporation, and)
UNIMANIA, INC., a)
Delaware corporation)
)
Defendants/Counterclaim)
Plaintiffs)

ORAL AND VIDEOTAPED DEPOSITION OF GARY WILCOX, Ph.D.
FEBRUARY 9, 2022

ORAL AND VIDEOTAPED DEPOSITION OF GARY WILCOX,
Ph.D. produced as a witness at the instance of the Plaintiff
and duly sworn, was taken in the above styled and numbered
cause on Wednesday, February 9, 2022, from 9:04 a.m. to
2:48 p.m., before Janalyn Elkins, CSR, in and for the
State of Texas, reported by computerized stenotype
machine, via Zoom, pursuant to the Federal Rules of Civil
Procedure and any provisions stated on the record herein.

<p style="text-align: right;">Page 158</p> <p>1 Q. So I take it you don't know whether that would</p> <p>2 have a corollary in traditional media analyses about</p> <p>3 competitive campaigns, right?</p> <p>4 A. I didn't understand that last question.</p> <p>5 Q. I said, if -- if you don't know what's being</p> <p>6 used, then you can't say that that would necessarily</p> <p>7 have a corollary in traditional media?</p> <p>8 A. Yeah. I honestly -- I don't know if they use</p> <p>9 that.</p> <p>10 Q. Right. But if they did, you -- you don't know</p> <p>11 whether that would be the same thing as what was being</p> <p>12 done before, right, because you just don't know what it</p> <p>13 is?</p> <p>14 A. Yeah, I don't know.</p> <p>15 MS. MEHTA: Why don't we go off the record?</p> <p>16 VIDEOGRAPHER: We're off the record at</p> <p>17 1:00 p m.</p> <p>18 (Brief recess.)</p> <p>19 VIDEOGRAPHER: We're back on the record at</p> <p>20 1:53 p m.</p> <p>21 Q. (BY MS. MEHTA) All right. Mr. Wilcox, welcome</p> <p>22 back. I wanted to follow up with you on some additional</p> <p>23 items. Would you agree with me that there are</p> <p>24 privacy-related concerns relating to consumers online</p> <p>25 targeted ad data?</p>	<p style="text-align: right;">Page 160</p> <p>1 [REDACTED]</p> <p>2 [REDACTED]</p> <p>3 [REDACTED]</p> <p>4 [REDACTED]</p> <p>5 [REDACTED]</p> <p>6 [REDACTED]</p> <p>7 [REDACTED]</p> <p>8 [REDACTED]</p> <p>9 [REDACTED]</p> <p>10 [REDACTED]</p> <p>11 [REDACTED]</p> <p>12 [REDACTED]</p> <p>13 [REDACTED]</p> <p>14 [REDACTED]</p> <p>15 [REDACTED]</p> <p>16 [REDACTED]</p> <p>17 [REDACTED]</p> <p>18 [REDACTED]</p> <p>19 [REDACTED]</p> <p>20 [REDACTED]</p> <p>21 [REDACTED]</p> <p>22 [REDACTED]</p> <p>23 [REDACTED]</p> <p>24 [REDACTED]</p> <p>25 [REDACTED]</p>
<p style="text-align: right;">Page 159</p> <p>1 A. What sorts?</p> <p>2 Q. Any.</p> <p>3 A. Are there any privacy concerns related to</p> <p>4 consumers targeting of ads?</p> <p>5 Q. Yeah, the online targeting of ads to consumers?</p> <p>6 A. Is there any -- yeah, I'm sure there's bound to</p> <p>7 be privacy concerns.</p> <p>8 Q. And would agree with me that platforms like</p> <p>9 Meta have an obligation to protect consumer privacy when</p> <p>10 it comes to targeted ad information?</p> <p>11 MR. TAYLOR: Object to form.</p> <p>12 THE WITNESS: I don't know if I agree with</p> <p>13 that or not.</p> <p>14 Q. (BY MS. MEHTA) You don't have an opinion on it</p> <p>15 one way or the other?</p> <p>16 A. Not really.</p> <p>17 Q. Would you agree with me that platform like Meta</p> <p>18 has a legitimate interest in trying to protect the</p> <p>19 consumer data that's on its platform?</p> <p>20 MR. TAYLOR: Object to form.</p> <p>21 THE WITNESS: What kind of consumer data?</p> <p>22 Q. (BY MS. MEHTA) Information about the user,</p> <p>23 their demographics for graphics, for example?</p> <p>24 A. Do they have an obligation to protect the</p> <p>25 consumer, is that what you're asking?</p>	<p>1 [REDACTED]</p> <p>2 [REDACTED]</p> <p>3 [REDACTED]</p> <p>4 [REDACTED]</p> <p>5 [REDACTED]</p> <p>6 [REDACTED]</p> <p>7 [REDACTED]</p> <p>8 [REDACTED]</p> <p>9 [REDACTED]</p> <p>10 [REDACTED]</p> <p>11 [REDACTED]</p> <p>12 [REDACTED]</p> <p>13 [REDACTED]</p> <p>14 [REDACTED]</p> <p>15 [REDACTED]</p> <p>16 [REDACTED]</p> <p>17 [REDACTED]</p> <p>18 [REDACTED]</p> <p>19 [REDACTED]</p> <p>20 [REDACTED]</p> <p>21 [REDACTED]</p> <p>22 [REDACTED]</p> <p>23 [REDACTED]</p> <p>24 [REDACTED]</p> <p>25 [REDACTED]</p>

Page 194

1 since then.

2 Q. Oh, fair enough. I guess what I meant is, have

3 you received anything about what his opinions are on the

4 technical issues since this report which was dated

5 March 2021?

6 A. I have not.

7 Q. Okay.

8 MS. MEHTA: All right. That's it. Thank

9 you.

10 MR. TAYLOR: Thank you, Professor Wilcox.

11 VIDEOGRAPHER: Janalyn, is there anything

12 you want to get on the record before we go off?

13 THE REPORTER: Dustin, if you want to tell

14 me your order.

15 MR. TAYLOR: We can do that off the record.

16 VIDEOGRAPHER: We're off the record

17 at 2:48 p m.

18 (Deposition concluded 2:48 p m.)

19

20

21

22

23

24

25

Page 195

1 REPORTER'S CERTIFICATION

2 DEPOSITION OF GARY WILCOX

3 TAKEN FEBRUARY 9, 2022

4 I, Janalyn Elkins, Certified Shorthand

5 Reporter in and for the State of Texas, hereby certify

6 to the following:

7 That the witness, GARY WILCOX, was duly sworn

8 by the officer and that the transcript of the oral

9 deposition is a true record of the testimony given by

10 the witness;

11 That the original deposition was delivered to

12 SONAL N. MEHTA;

13 That a copy of this certificate was served on

14 all parties and/or the witness shown herein on

15 _____.

16 I further certify that pursuant to FRCP No.

17 30(f)(i) that the signature of the deponent was not

18 requested by the deponent or a party before the

19 completion of the deposition.

20 I further certify that I am neither counsel

21 for, related to, nor employed by any of the parties in

22 the action in which this proceeding was taken, and

23 further that I am not financially or otherwise

24

25

Page 196

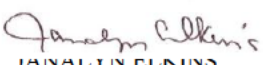
1 interested in the outcome of the action.

2 Certified to by me this 9th day of February

3 2022.

4

5

6 
 JANALYN ELKINS
 Texas CSR 3631
 Expiration Date 1/31/2023
 Veritext Legal Solutions
 300 Throckmorton Street, Suite 1600
 Fort Worth, Texas 76102
 Firm Registration No. 571
 PH: (817) 336-3042

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

Page 197

1 Meta Platforms, Inc. v. Brandtotal, LTD., et al.

2 Gary Wilcox, Ph.D. (#5081374)

3 E R R A T A S H E E T

4 PAGE ____ LINE ____ CHANGE _____

5 _____

6 REASON _____

7 PAGE ____ LINE ____ CHANGE _____

8 _____

9 REASON _____

10 PAGE ____ LINE ____ CHANGE _____

11 _____

12 REASON _____

13 PAGE ____ LINE ____ CHANGE _____

14 _____

15 REASON _____

16 PAGE ____ LINE ____ CHANGE _____

17 _____

18 REASON _____

19 PAGE ____ LINE ____ CHANGE _____

20 _____

21 REASON _____

22 _____

23 _____

24 Gary Wilcox, Ph.D. Date _____

25

Page 198

1 Meta Platforms, Inc. v. Brandtotal, LTD., et al.

2 Gary Wilcox, Ph.D. (#5081374)

3 ACKNOWLEDGEMENT OF DEPONENT

4 I, Gary Wilcox, Ph.D., do hereby declare that I

5 have read the foregoing transcript, I have made any

6 corrections, additions, or changes I deemed necessary as

7 noted above to be appended hereto, and that the same is

8 a true, correct and complete transcript of the testimony

9 given by me.

10

11 _____

12 Gary Wilcox, Ph.D. Date

13 *If notary is required

14 SUBSCRIBED AND SWORN TO BEFORE ME THIS

15 _____ DAY OF _____, 20____.

16

17

18

19 _____
NOTARY PUBLIC

20

21

22

23

24

25

51 (Page 198)

Veritext Legal Solutions

215-241-1000 ~ 610-434-8588 ~ 302-571-0510 ~ 202-803-8830

EXHIBIT 15

Unimania, Inc. Privacy PolicyLast updated: *March 31, 2020***Privacy Policy**

This Privacy Policy governs how we, Unimania, Inc. and our affiliates (“**Unimania**”, “**we**”, “**our**” or “**us**”), use data that we collect, receive and store in connection with your use of Unimania’s software applications (collectively referred to herein as the “**Software**”). We use, collect and store personal data we collect or receive from or about you (“**you**”) such as in the following use case:

- When you contact us (e.g. customer support, need help, submit a request) at: privacy@unimania.xyz

The data that we collect in connection with our Software is automatically rendered anonymized and non-personal. We do not collect or store any of your personal data (unless you decide to contact us with a question as specified above), nor do we ever monitor or track your personal activities, apart from clicks that you may have initiated on sponsored ads in an anonymized manner.

Important note: Nothing in this Privacy Policy is intended to limit in any way your statutory right, including your rights to a remedy or means of enforcement.

Table of contents:

- [The Data that We Collect, Why We Collect it, and How it is Used](#)
- [Why We Collect and Process the Data](#)
- [How We Protect And Retain Your Information](#)
- [How We Share Data Your Data. Additional Information Regarding Transfers Of Personal Data](#)
- [Your Privacy Rights. How To Delete Your Account](#)
- [US privacy provisions](#)
- [Use by children](#)
- [Interaction With Third Party Products](#)
- [Contact Us](#)

This Privacy Policy may be updated from time to time and therefore we ask you to check back periodically for the latest version of the Privacy Policy.

The Data that We Collect, Why We Collect it, and How it is Used

We collect the following data:

Data We Collect	Sources - where we obtain the personal data from (CCPA only, if applicable)	Why is the data collected and for what purposes?	Legal basis for data collection(GDPR only, if applicable)	Third Parties with whom we Share your Data	Consequences of not providing the data
Full name Email address Any other information that you decide to provide/supply us	We collect this information from you	To answer your questions To communicate with you by email.	Necessary to perform a contract or take steps, at your request, to enter into a contract. Legitimate interest (e.g., to answer your	Gmail for Business.	We will not be able to respond to your specific request.

			questions).		
--	--	--	-------------	--	--

- (1) **Collection of Non-Personal, Statistical Data.** We collect data about sponsored campaigns, sponsored posts or advertisements that target you directly or that have been shared with you in your social feed, including clicks that you may have initiated on such ads. We complement these data with your anonymized user ID general, as well as general browser and operating system information that we collect from your browser user agent, such as: demographic information like your age, your gender, where you live (by region), your relationship status and your general interests, as stored by social networks (“Demographic Information”), if such available. Upon collection of the Demographic Information, The Software immediately anonymizes such Demographic Information using a mathematical function known as “hash function”, after which it is transferred to us. Demographic Information that has been hashed cannot be traced back to you or any other user and does not enable identification of an individual person.
- (2) **Log Files.** Log files are automatically created as a result of errors in the code of the Software that are stored in log entries. Such log files contain information like your internet protocol (IP) address, browser type, internet service provider (ISP) and any other information the browser automatically sends. We do not control the log files transmitted and we do not store or use these log files
- (3) **Analytics Tools**
 - **Google Analytics.** The Website uses a tool called “Google Analytics” to collect information about use of the Website. Google Analytics collects information such as how often users visit this Website, what pages they visit when they do so, and what other websites they used prior to coming to this Website. We use the information we get from Google Analytics to maintain and improve the Website and our products. We do not combine the information collected through the use of Google Analytics with personal information. Google’s ability to use and share information collected by Google Analytics about your visits to this Website is restricted by the Google Analytics Terms of Service, available at <https://marketingplatform.google.com/about/analytics/terms/us/>, and the Google Privacy Policy, available at <http://www.google.com/policies/privacy/>. You may learn more about how Google collects and processes data specifically in connection with Google Analytics at <http://www.google.com/policies/privacy/partners/>. You may prevent your data from being used by Google Analytics by downloading and installing the Google Analytics Opt-out Browser Add-on, available at <https://tools.google.com/dlpage/gaoptout/>.
 - **Firebase Analytics.** We also use “Google Analytics for Firebase”. By enabling this tool, we enable the collection of data about App Users, including via identifiers for mobile devices (including Android Advertising ID and Advertising Identifier for iOS), cookies and similar technologies. We use the information we get from Google Analytics for Firebase to maintain and improve our App(s). We do not facilitate the merging of personally-identifiable information with non-personally identifiable information unless we have robust notice of, and your prior affirmative (i.e., opt-in) consent to, that merger. Finally, please note that Google Analytics for Firebase’s terms (available at <https://firebase.google.com/terms/>) shall also apply.
 - **AppsFlyer.** We use a tool called “AppsFlyer”, a mobile attribution and marketing analytics platform to understand the use of our services. AppsFlyer is exposed to the following data: (i) unique identifiers and technical data, such as IP address, User agent, IDFA (Identifier For Advertisers) or Android ID (in Android devices); and (ii) technical data regarding your operating system, device attributes and settings, applications, advertising opt-out signals, Google Advertiser ID, in-app events, device motion parameters and carrier. The use of this data allows us to analyze our campaigns and performance, as well as your habits and characteristics. For example, the data AppsFlyer receives includes downloads, impressions, clicks and installations of their mobile applications, mobile device use and data regarding in-app events. AppsFlyer’s terms of use (available at <https://www.appsflyer.com/terms-of-use/>) and privacy policy (available at <https://www.appsflyer.com/privacy-policy/>) also apply to the use of AppsFlyer.
- (4) **Location Data.** The Software uses a tool called MaxMind to obtain certain location-based data in connection with your use of the Software, transmitted from your Facebook account and your IP address. We use such location-based data only to determine high-level region, state and country level location data which we store and use. We never store or use your IP address or any other specific location-based data. You may learn more about how MaxMind collects and processes data at: <https://www.maxmind.com/en/privacy-policy>.

Why We Collect and Process the Data

- (1) We use the anonymized data that we collect, receive and store in connection with the Software (as described in this Privacy Policy) to analyze how companies promote their products and services online and on social networks and to what groups of people (i.e. target groups). We provide our customers with data intelligence and insights into their advertising practices as well as those of their competitors. Therefore, the data we share with them is always aggregated and non-personal.
- (2) **Do we identify you with the data we collect? No.** We, along with our affiliates, provide market research solutions, and, therefore, any data that we collect is automatically rendered **anonymized and non-personal**, so there is no way to actually identify you or others. If you decide to contact us with a question or inquiry, we will only use the information that you provide to us in order to respond to you, and for no other purpose.

How we Protect and Retain your Information

- (1) **Security.** We have implemented appropriate technical, organizational and security measures designed to protect your personal data. However, please note that we cannot guarantee that the information will not be compromised as a result of unauthorized penetration to our servers. As the security of information depends in part on the security of the computer, device or network you use to communicate with us and the security you use to protect your user IDs and passwords, please make sure to take appropriate measures to protect this information.
- (2) **Retention of your personal data.** Your Personal Data will be stored until: (i) we no longer need the information and proactively delete it; or (ii) you send a valid deletion request. Please note that we will retain it for a longer or shorter period in accordance with data retention laws. In addition in some circumstances we may store your personal data for longer periods of time, for example (i) where we are required to do so in accordance with legal, regulatory, tax or accounting requirements, or (ii) for us to have an accurate record of your dealings with us in the event of any complaints or challenges, or (iii) if we reasonably believe there is a prospect of litigation relating to your personal data or dealings. We have an internal data retention policy to ensure that we do not retain your personal data perpetually.

How We Share Data Your Data; Additional Information Regarding Transfers Of Personal Data.

We share the data that we collect in the following ways:

- (1) We store and process the data on servers at Amazon Web Services (AWS) - United States and Microsoft Azure facilities in the United Kingdom.
- (2) **Internal transfers:** Transfers within the Unimania Group will be covered by an internal processing agreement entered into by members of the Unimania Group (an intra-group agreement) which contractually obliges each member to ensure that personal data receives an adequate and consistent level of protection wherever it is transferred to.
- (3) **External transfers:** Where we transfer your personal data outside of EU/EEA (for example to third parties who provide us with services), we will obtain contractual commitments from them to protect your personal data. Some of these assurances are well recognized certification schemes like the EU - US Privacy Shield for the protection of Personal Data transferred from within the EU to the United States.
- (4) To comply with all applicable laws, regulations and rules, and requests of law enforcement, regulatory and other governmental agencies or if required to do so by court order.
- (5) In the event that we are acquired by, or merged with, a third party entity, or in the event of bankruptcy or a comparable event, we reserve the right to transfer, disclose or assign your personal data in connection with the foregoing events; and/or
- (6) Where you have provided your consent to us sharing or transferring your personal data (e.g., where you provide us with consents or opt-in to optional additional services or functionality).
- (7) If, in the future, we sell or transfer, or we consider selling or transferring, some or all of our business or assets to a third party, we will (to the extent required) disclose, transfer or assign information to such third party purchaser,

including, if required, the anonymized, non-personal data, subject to its compliance with this Privacy Policy. In the event of bankruptcy or a comparable event, we reserve the right to disclose, transfer or assign data in connection with the foregoing events.

If you want to receive the list of the current recipients of your personal data, please make your request by contacting us to privacy@unimania.xyz.

Your Privacy Rights

(1) **GDPR Data Subject Rights.** The following rights (which may be subject to certain exemptions or derogations) shall apply to certain individuals (some of which only apply to individuals protected by the GDPR):

- You have the right to know what personal information is being collected about you;
- You have a right to access personal data held about you. Your right of access may normally be exercised free of charge, however we reserve the right to charge an appropriate administrative fee where permitted by applicable law;
- You have the right to request that we rectify any personal data we hold that is inaccurate or misleading;
- You have the right to request the erasure/deletion of your personal data (e.g. from our records and the records of our service providers). Please note that there may be circumstances in which we are required to retain your personal data, for example for the establishment, exercise or defense of legal claims;
- You have the right to object, to or to request restriction, of the processing;
- You have the right to data portability. This means that you may have the right to receive your personal data in a structured, commonly used and machine-readable format, and that you have the right to transmit that data to another controller;
- You have the right to object to profiling;
- You have the right to know whether your personal information is sold or disclosed and to whom;
- You have the right to say no to the sale of your personal information;
- You have the right to withdraw your consent at any time. Please note that there may be circumstances in which we are entitled to continue processing your data, in particular if the processing is required to meet our legal and regulatory obligations. Also, please note that the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal;
- You also have a right to request certain details of the basis on which your personal data is transferred outside the European Economic Area, but data transfer agreements and/or other details may need to be partially redacted for reasons of commercial confidentiality;
- You have the right to equal service and price, even if you exercise your privacy rights;
- You have a right to lodge a complaint with your local data protection supervisory authority (i.e., your place of habitual residence, place of work or place of alleged infringement) at any time or before the relevant institutions in your place of residence (e.g. the Attorney General in your State). We ask that you please attempt to resolve any issues with us before you contact your local supervisory authority and/or relevant institution.

(2) **CCPA Consumer Rights** The following rights (which may be subject to certain exemptions or derogations) shall apply to certain individuals (some of which only apply to individuals protected by the CCPA):

- You have the right to know what personal information is being collected about you;
- You have the right to request the erasure/deletion of your personal data (e.g. from our records and the records of our service providers). Please note that there may be circumstances in which we are required to retain your personal data, for example for the establishment, exercise or defense of legal claims;
- You have the right to know whether your personal information is sold or disclosed and to whom;
- You have the right to say no to the sale of your personal information;
- You have the right to equal service and price, even if you exercise your privacy rights;
- You have a right to lodge a complaint with your local data protection supervisory authority (i.e., your place of habitual residence, place of work or place of alleged infringement) at any time or before the relevant institutions in your place of residence (e.g. the Attorney General in your State). We ask that you please attempt to resolve any issues with us before you contact your local supervisory authority and/or relevant institution

(3) **Exercising your Rights.** You can exercise your rights by contacting us at privacy@unimania.xyz or, if you are an individual protected by CCPA, via the “contact us” button on each of our apps. You may also request to utilize some of your rights under CCPA using an authorized agent, if the person is registered with the California Secretary of State and you provided it with a written permission to act on your behalf. In some cases we may ask you additional information to verify the identity of the requestor of your CCPA privacy right(s).

Subject to legal and other permissible considerations, we will make every reasonable effort to honor your request promptly in accordance with applicable law or inform you if we require further information in order to fulfil your request. When processing your request, we may ask you for additional information to confirm or verify your identity and for security purposes, before processing and/or honoring your request. We reserve the right to charge a fee where permitted by law, for instance if your request is manifestly unfounded or excessive, but in any event, under no circumstances will we discriminate against you for exercising any of your CCPA rights.

In the event that your request would adversely affect the rights and freedoms of others (for example, would impact the duty of confidentiality we owe to others) or if we are legally entitled to deal with your request in a different way than initially requested, we will address your request to the maximum extent possible, all in accordance with applicable law.

For more information or for exercising your rights, please contact us at privacy@unimania.xyz. Subject to legal and other permissible considerations, we will make every reasonable effort to honor your request promptly or inform you if we require further information in order to fulfil your request.

Us Privacy Provisions

- (1) Access Requests. California Civil Code Section 1798.83 permits our customers who are California residents to request certain information regarding our disclosure of Personal Data to third parties for their direct marketing purposes. To make such a request, please send an email to privacy@unimania.xyz. Please note that we are only required to respond to one request per customer each year.
- (2) Our California Do Not Track Notice. We do not track users over time or across third party websites and therefore do not respond to Do Not Track signals. We do not allow third parties to collect personally identifiable information about an individual user's online activities over time and across different web sites when a user uses the Website.
- (3) Deletion of Content from California Residents. If you are a California resident under the age of 18 and a registered user, California Business and Professions Code Section 22581 permits you to remove content or Personal Data you have publicly posted. If you wish to remove such content or Personal Data and you specify which content or Personal Data you wish to be removed, we will do so in accordance with applicable law. Please be aware that after removal you will not be able to restore removed content. In addition, such removal does not ensure complete or comprehensive removal of the content or Personal Data you have posted and that there may be circumstances in which the law does not require us to enable removal of content.
- (4) CCPA Sale of personal information; Disclosure of personal information for business purposes. We do not sell any personal information and we do not disclose any personal information of Users for any business purpose, other than as described herein. Accordingly, we have not sold or disclosed consumers' personal information for a business purpose in the preceding 12 months.
- (5) Information collected in the last 12 months is described above. If you have further questions with respect to the collection, use, disclosure or sale of your personal information (if any), please make your request by contacting us to privacy@unimania.xyz.

Use by Children

We do not offer our Software for use by children. If you are under 18, you may not use the Software, or provide us with any information without involvement of a parent or a guardian. For the purposes of the GDPR, we do not intend to *offer information society services directly to children*. In the event that we become aware that you provide personal data in violation of applicable privacy laws, we reserve the right to delete it. We do not knowingly collect personal information from, and/or about children. If you believe that we might have any such personal information, please contact us at privacy@unimania.xyz.

Interaction With Third Party Products

We enable you to interact with third party websites, mobile software applications and products or services that are not owned or controlled by us (each a "**Third Party Service**"). We are not responsible for the privacy practices or the content of such Third Party Services. Please be aware that Third Party Services can collect Personal Data from you. Accordingly, we encourage you to read the terms and conditions and privacy policies of each Third Party Service.

Contact Us

If you have any questions, concerns or complaints regarding our compliance with this notice and the data protection laws, or if you wish to exercise your rights, we encourage you to first contact us at privacy@unimania.xyz.

EXHIBIT 16

EXHIBIT FILED UNDER
SEAL

EXHIBIT 17

1
2
3
4
5
6
7
8 **UNITED STATES DISTRICT COURT**
9 **NORTHERN DISTRICT OF CALIFORNIA**
10 **SAN FRANCISCO DIVISION**

11 FACEBOOK, INC., a Delaware corporation,

12 Plaintiff,

13 v.

14 BRANDTOTAL LTD., an Israeli corporation,
15 and UNIMANIA, INC., a Delaware
corporation,

16 Defendants.
17
18
19
20
21
22
23
24
25
26
27
28

Case No. 3:20-CV-07182-JCS

**DECLARATION OF SANCHIT KARVE IN
SUPPORT OF PLAINTIFF'S OPPOSITION
TO DEFENDANTS' *EX PARTE* MOTION
FOR A TEMPORARY RESTRAINING
ORDER**

DECL. OF SANCHIT KARVE

1 I, Sanchit Karve, declare:

2 1. I submit this declaration in support of Plaintiff Facebook, Inc.'s ("Facebook")
3 Opposition in the above-captioned matter. I have personal knowledge of the facts set forth herein,
4 and if called to testify as a witness, I could do so competently under oath.

5 2. I have a Bachelor's and Master's degree in computer science. I have professional
6 experience in malware analysis, including reverse engineering malware.

7 3. I am employed by Facebook as a Malware Researcher on the eCrime team at
8 Facebook. I have been employed by Facebook since 2018. My responsibilities as a Malware
9 Researcher include identifying types of malware (*e.g.* ransomware, banking Trojan, keylogger, data
10 scraper), malware vulnerabilities (*e.g.* method used to obtain access to the targeted computer), the
11 infrastructure used by the malware (*e.g.* servers, IP addresses, domain names), and malware
12 functionality (*e.g.* steal login credentials, banking information). On the eCrime team, I also have
13 access to Facebook and Instagram account and administrative records.

14 **I. Unimania and BrandTotal Extensions and Apps**

15 4. In or around April 2020, I began investigating multiple browser extensions on the
16 Google Chrome Store believed to be scraping data from Facebook and Instagram.

17 5. Since April 2020, I have investigated and researched the activities of the following
18 browser extensions (a and b) and app (c) developed by or controlled by BrandTotal and Unimania:

- 19 a. UpVoice
- 20 b. Ads Feed
- 21 c. Anonymous Story Viewer for Instagram

22 6. I also reviewed a report published by the co-founder of AdGuard (attached as
23 Exhibit 1) that assessed the activities of the following browser extensions that AdGuard identified as
24 being used by Unimania to harvest data from Facebook:

- 25 a. Video Downloader for Facebook
- 26 b. Album & Photo Manager for Facebook
- 27 c. PDF Merger – PDF Files Merger
- 28 d. Pixcam – Webcam Effects

1 7. The UpVoice and Ads Feed and the extensions identified in paragraph 6 were
2 available for download through the Google Chrome Store. As of October 18, 2020, the Anonymous
3 Story Viewer for Instagram app was available for download from the Google Play store. I identified
4 multiple versions of the Ads Feed and UpVoice extensions from the Google Chrome Store. A new
5 version of an extension usually means something in the code of the extension was changed.

6 8. Internet browsers, such as Google Chrome, Opera, and Mozilla Firefox, are used to
7 access the internet. Internet browsers follow instructions from websites, in computer code, to render
8 and display a website's content for users to see. Website content is largely delivered in HTML code.
9 Internet browsers are designed to render the HTML code and display it in images and text for the
10 user's screen.

11 9. Internet browser extensions are software components that alter a browser's
12 functionality. Browser extensions can be installed to enhance user experience and the functionality
13 of the browser. For example, a browser extension can block pop-up ads.

14 10. Browser extensions can also be used in illicit ways. Browser extensions can be coded
15 to access the full array of information available to the browser and its functionalities. For example, a
16 browser extension can be designed to monitor a user's browsing session, manipulate how the content
17 of visited websites is displayed, and take other unauthorized actions.

18 11. A mobile app, like Anonymous Story Viewer for Instagram, is a computer program
19 designed to run on a mobile or tablet that provide the user with a function or service.

20 12. As a part of my investigation, I downloaded and reviewed the Ads Feed and UpVoice
21 extensions. Included in each download was a ZIP file that contained the extensions' JavaScript
22 source code. By reviewing that source code, I was able to understand how each extension worked
23 and the functionality of each extension. I also reviewed a technical analysis of the app --
24 Anonymous Story Viewer for Instagram - prepared by the Facebook External Data Misuse ("EDM")
25 team. EDM's technical analysis was prepared after downloading the app from the Google Play Store
26 and reviewing its code and testing the app.

27 13. The UpVoice and Ads Feed extensions and the Anonymous Story Viewer for
28 Instagram app are automated scraping tools. Once installed by a user, the extensions and app were

1 coded to automatically scrape information and data without the user having to do anything other than
2 visit the website targeted for scraping. To accomplish this, the extensions and app were coded to
3 exploit the legitimate user's browser as a proxy to access password-protected information on
4 Facebook and Instagram and request data while pretending to be an authenticated Facebook or
5 Instagram user with legitimate login credentials. This method of scraping allowed BrandTotal and
6 Unimania to access password-protected locations on Facebook's computers and obfuscate the
7 extensions' and app's activity from Facebook and Instagram.

8 **II. Information Scraped by BrandTotal and Unimania Extensions and App**

9 **A. UpVoice Browser Extension**

10 14. I reviewed multiple versions of the UpVoice extension that were available between
11 April 2020, and October 2020. On October 1, 2020 the UpVoice extension was removed from the
12 Google Chrome store. On October 12, 2020, I learned that a new extension named "UpVoice" was
13 publicly accessible on the Chrome Store. Exhibit 2. That version of the extension was removed
14 from the Chrome Store on or about October 14, 2020 and published again that same day. Exhibit 3.
15 It remained on the Google Chrome Store until on or about October 18, 2020. At the time it was
16 removed, information on the Chrome Store showed it had been downloaded at least 150 times.
17 Based on my analysis of the version of the UpVoice extension made available on October 12, 2020
18 (see Exhibit 2), that version of the extension was operational at that time and it exfiltrated data and
19 information from Facebook's computers.

20 15. Once a user installed the UpVoice extension, the extension used the user's browser as
21 a proxy to access Facebook computers and request data from Facebook while pretending to be an
22 authenticated Facebook user with legitimate login credentials. This method of scraping allowed
23 BrandTotal and Unimania to access password-protected areas on Facebook's computers and
24 obfuscates the extension's activity from Facebook.

25 16. With respect to the collection of Facebook data, each version of the UpVoice
26 extension that I reviewed was functionally identical. Each worked in a similar way and was coded to
27 scrape the same information from Facebook computers. Based on my review of the UpVoice
28

1 extension, I concluded it violates section 3.2.3 of the Facebook Terms of Service, which prohibits
2 accessing or collecting data using automated means without Facebook's permission.

3 17. To the best of my knowledge, each version of the UpVoice extension that I reviewed
4 scrapes, has scraped, or was coded to scrape the following information and data from Facebook's
5 computers when a user who had installed the extension visited the Facebook platform:

6 a. User profile information. The versions of the UpVoice extension that I
7 reviewed were coded to scrape data and information from users' Facebook profiles, including their
8 Facebook user IDs, gender, date of birth, self-disclosed location, and relationship status. A user's
9 Facebook ID is a unique identification number that is associated with that user's Facebook account.
10 Depending on the user's profile privacy settings, a user's date of birth, self-disclosed location, and
11 relationship status can be publicly viewable or private, but the versions of the UpVoice extension
12 that I reviewed were coded to scrape that information regardless of the user's privacy settings.
13 Additionally, I determined that the user profile information was scraped even if the user did not
14 access the profile settings where this information was located.

15 b. Advertising interests. Every Facebook user profile contains Ad Preference
16 information that includes the user's advertising interests by category. Ad Preference information is
17 not publicly viewable but is accessible to the authenticated Facebook user through their profile
18 settings. The versions of the UpVoice extension that I reviewed were coded to scrape user
19 advertising-interest categories from its non-publicly viewable location in user settings.

20 Categories of advertising interests can include, for example, "Parenting," "Home
21 Improvement," or "Shopping," but they can also be more specific. Facebook generates these
22 categories of interests based on a user's activities on Facebook. Clicking on advertisements for
23 children's products, for example, may result in the "Parenting" category being added to a user's list
24 of advertising interests. Users can access and opt-out of categories if they no longer wish to see
25 advertisements of that type. Facebook uses this information internally to determine what
26 advertisements to display to a particular user. Individual users can access information about their
27 own advertising interests while they are logged into their Facebook account. But the information
28 cannot be accessed by anyone other than the individual user and Facebook's internal systems.

1 c. Advertisements. The versions of the UpVoice extension that I reviewed were
2 coded to scrape information about advertisements viewed by users who had installed the extension,
3 including an advertisement's text, images or videos, buttons that users can click to navigate to other
4 webpages, and data on who sponsored the advertisements, all from a non-publicly viewable location
5 on Facebook. The versions of the UpVoice extension I reviewed were also coded to scrape the
6 Uniform Resource Locator or "URL" associated with every aspect of an advertisement and any "call
7 to action" buttons (e.g. "click here") that the advertisement contained. The URLs provided the
8 addresses to permanent webpages that contain the images used in the advertisements or the website
9 linked through the buttons on those advertisements. URLs for full advertisements from a user's New
10 Feed were only available to authenticated Facebook users. The URLs scraped by the UpVoice
11 extension enable users and non-users to view advertisements and advertising metrics (discussed below
12 in section II.A.(d)) even after the advertisement became inactive at the end of its campaign duration.

13 d. Advertising Metrics. Facebook users can engage with an advertisement in
14 various ways, including by commenting on it, sharing it, or reacting to it using Facebook's
15 prepopulated reactions—thumbs up, heart, a laughing face, a surprised face, a sad face, and an angry
16 face. Only authenticated users can comment, share, or react to an advertisement. For any
17 advertisement viewed by a Facebook user who installed the UpVoice extension, the UpVoice
18 extension scraped the number of comments, reactions, shares associated with the advertisement.
19 These advertising metrics are not publicly viewable in the Ads Library. These metrics are viewable
20 to other authenticated Facebook users on Facebook and non-users who have access to the
21 advertisement's URL scraped by the UpVoice extension.

22 e. Instagram. Certain versions of the UpVoice extension that I reviewed were
23 also coded to scrape data from Instagram. Those versions were coded to automatically scrape
24 certain data from Instagram when a user who installed the extension visited Instagram. The
25 extension was coded to scrape the Instagram user's name, account name, user ID, and profile picture
26 and, similar to the way it scraped data from Facebook, advertisements and advertising metrics. I
27 could not identify anything in the extension's code that anonymized the user profile information that
28 was scraped. The most recent version of the UpVoice extension did not scrape data from Instagram.

B. Ads Feed Browser Extension

18. I reviewed multiple versions of the Ads Feed extension. The Ads Feed extension was removed from the Google Chrome Store on October 1, 2020. Based on my review of the source code for the Ads Feed extension, I determined that all the versions of the extension I reviewed used code almost identical to the UpVoice extensions that I reviewed. The Ads Feed extensions I reviewed were also coded to scrape data from Instagram.

19. Like the UpVoice extensions that I reviewed, once a user installed the Ads Feed extension, the extension used the user's browser as a proxy to access Facebook computers and request data from Facebook while pretending to be an authenticated Facebook user with legitimate login credentials. This method of scraping allowed BrandTotal and Unimania to access password-protected areas on Facebook's computers and obfuscates the extension's activity from Facebook.

20. As to Facebook, the Ads Feed extension was coded to scrape the same user profile information, advertisements and advertising metrics, and Ad Preference information as the UpVoice extension. As to Instagram, the extension was coded to scrape the same information from Instagram as earlier versions of the UpVoice extension.

21. The data scraped by the Ads Feed extension was sent to the same servers as the data collected through the UpVoice malicious extension.

C. Anonymous Story Viewer for Instagram

22. In early October 2020, the Facebook EDM team downloaded and reviewed the Anonymous Story Viewer for Instagram app from the Google Play store. Unimania is listed as the developer of that app. Based on their analysis of the app, as of April 15, 2020, the app was scraping, from a user who installed the app and visited Instagram, the Instagram users ID, name of the user, phone number, email address, gender profile picture, Instagram accounts followed by the user and the name of the Instagram accounts following the user, the user's posts, and the comments and captions for posts, the URL for the posts, and the geotag of the Instagram post which is information embedded in the metadata of the photo that shows where the photo in the post was taken. None of the information was anonymized and was sent to a third-party server in plain text.

1 23. The app was also coded to scrape the session token and the user's session ID. This
2 information was exfiltrated to a third-party server as well. Anyone who possessed the session token
3 and session ID could make requests to Facebook computers for Instagram content for that user
4 without the user accessing Instagram.

5 **D. Ad Guard Report**

6 24. On May 30, 2018, AdGuard released a report analyzing what it identified to be four
7 browser extensions being used by Unimania to collect data. Exhibit 1. According to their website,
8 AdGuard is a software company focused on technology used to block ads on the internet. According
9 to the AdGuard report, the extensions they reviewed were coded to scrape data from Facebook
10 immediately after a user who installed one of the browser extensions opened their Internet browser.
11 Like the data scraped by the UpVoice and Ads Feed extensions, the data scraped by the extensions
12 discussed in the AdGuard report included data from a non-publicly viewable (*i.e.* password
13 protected) location on Facebook, and included a user's advertising interests, Facebook ID, and
14 advertisements.

15 25. According to the Ad Guard report, the extensions attempted to anonymize the user's
16 Facebook ID being scraped with a "static salt." The static salt replaced the user's Facebook ID—the
17 number associated with their Facebook profile—with a different set of unique numbers. Although
18 the Facebook user ID was no longer viewable as plain text, the static salt was a very weak form of
19 anonymization protection. It could be reversed very quickly, likely in under a minute, using publicly
20 available programs. The AdGuard published the instructions for reverse engineer the static salt used
21 by Unimania. Exhibit 1. By reverse engineering the static salt, anyone would have been able to
22 determine the Facebook ID number associated with the information scraped by those extensions.
23 The Facebook user ID could then be used to view the Facebook profile of the associated user and
24 connect the user to the information scraped by the extensions.

25 26. According the Ad Guard report, the data scraped through the extensions discussed in
26 the report was sent to the same servers as the data collected through the UpVoice and Ads Feed
27 extension that I reviewed. Policy statements in shown in the AdGuard report list Unimania as the
28 recipient of the data.

Facebook Accounts Associated with BrandTotal

27. I have viewed Facebook's and Instagram's user-account records for the accounts associated with Defendants.

28. Instagram account #####09355 ("Account 1") was created on December 6, 2016, uses the name "BrandTotal" and the username "brandtotal," and registration email address oren@brandtotal.io. Account 1 later changed their email address to social@brandtotal.io. Account 1 was disabled by Instagram on September 30, 2020.

29. Facebook account #####15996 ("Account 2") was created on June 13, 2017, uses the name "BrandTotal Analytics," and the registration email address social@brandtotal.io which is the same email address most recently used by Account 1. On June 13, 2017, Account 2 created Facebook Page #####52366 ("Page 1"), named it "BrandTotal," and used it to promote BrandTotal's marketing service. Page 1 and Account 2 were disabled by Facebook on September 30, 2020.

30. Facebook business account #####12689 ("Business 1") was created on February 21, 2017, using the name "BrandTotal." Page 1 was added as an asset to Business 1 giving it ownership on August 6, 2017. Business 1 owned one Facebook advertising account which promoted Page 1.

Accounts Associated With UpVoice

31. Facebook business account #####46916 ("Business 2") was created on September 3, 2019, using the name "UpVoice." Business 2 owned two Facebook advertising accounts which promoted Facebook Page #####68029 ("Page 2") named "UpVoice." Page 2, created January 24, 2019, was used to promote UpVoice's extensions and directed viewers to external website "joinupvoice.com." Business 1 owned two Facebook advertising accounts which promoted Page 2. Page 2 was disabled on September 30, 2020.

32. Facebook business account #####86182 ("Business 3") was created on June 8, 2020, using the name "UpVoice US." Page 2 was added as an asset to Business 3 giving it ownership on June 8, 2020. Business 3 owned one Facebook advertising account which promoted Page 2.

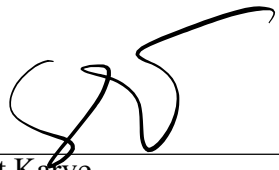
Accounts Associated With Unimania

33. Facebook business account #####61051 ("Business 4") was created on July 4, 2018, using the name "Unimania." Business 4 owned one Facebook advertising account which promoted Facebook Page #####47488 ("Page 3"). Page 3 was created on July 30, 2018, using the name "Ads Feed," was added as an asset to Business 4 on July 30, 2018, and was used to promote Unimania's extension. Page 3 was disabled on September 30, 2020.

New Facebook and Instagram Accounts

34. On October 3, 2020, Facebook account #####68025 was created using the name "Jack Buch" ("Account 4"). A few minutes later, Instagram account #####37627 was created using the name "Jack_Back" and username "Jackb696" ("Account 5"). Based on my review of Account 4 and Account 5, I determined those accounts were created by the same user who created Facebook account #####73211 ("Account 6"). Account 6 was created on April 20, 2008, using the name "Oren Dor." Based on publicly available information from the BrandTotal website, I know Oren Dor to be BrandTotal's Chief Product Officer. Account 4 was disabled on October 16, 2020. Account 5 was disabled on October 18, 2020. Account 6 was disabled on September 30, 2020.

I declare under penalty of perjury that the foregoing is true and correct. Executed at Mountain View, CA, on the 21st day of October, 2020.



Sanchit Karve

EXHIBIT 1

[Blog](#) > Unimania: I Need Your Facebook Data, Location, And Your Browsing History

Unimania: I Need Your Facebook Data, Location, And Your Browsing History

Privacy protection is basically what we do, so I never get tired of stories about how unpredictable the ways of getting Facebook user data are. Cambridge Analytica might be dead, but the business of stealing users' data lives on, and this article demonstrates one more example of that.

The story begins with the recent research I conducted about [fake ad blockers](#) in the Chrome Web Store. The outcome of that research was that I received dozens of questions about whether this or that extension is safe to use. This made me take a deeper look into the most popular Chrome extensions, but even so, I had no idea at that time where this investigation was going to lead me. In fact, it exposed to me a huge spyware campaign that utilizes popular Android apps and Chrome extensions to steal Facebook data and the browsing histories of millions of users.

Suspicious Chrome extensions

I conducted an automated scan of all publicly available Chrome extensions. This scan flagged quite a few different privacy issues, which I will address in more specific detail in a forthcoming post.

One of the issues that immediately caught my attention, as I noticed suspicious requests made to various Facebook domains.

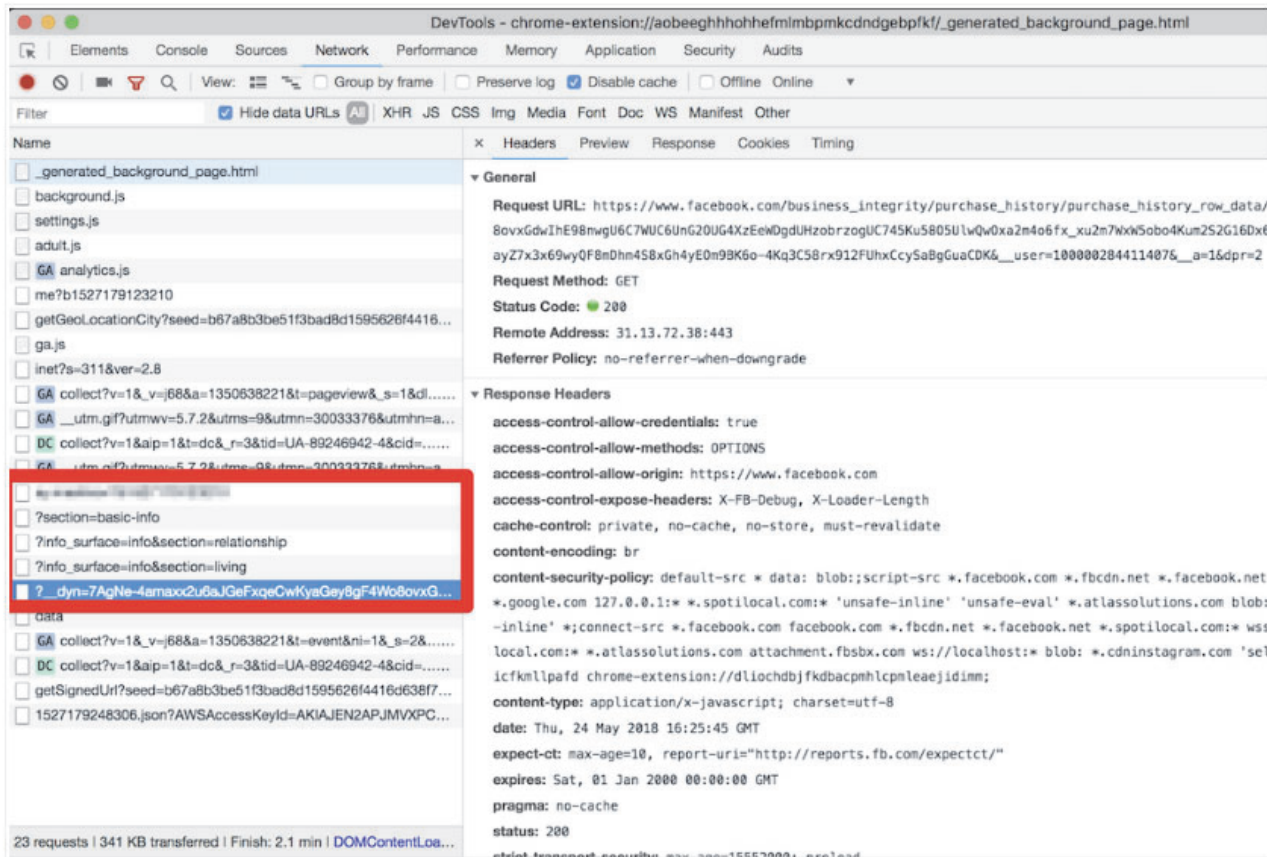
Meet these nasty Chrome extensions, currently in use by an estimated 420,000 users:

- [Video Downloader For Facebook](#) (170K+ users, [archived copy](#))
- [Album & Photo Manager For Facebook](#) (92K+ users, [archived copy](#))
- [PDF Merge - PDF Files Merger](#) (125K+ users, [archived copy](#))
- [Pixcam - Webcam Effects](#) (31K+ users, [archived copy](#))

So, what is wrong with them? Let's dive into the details.

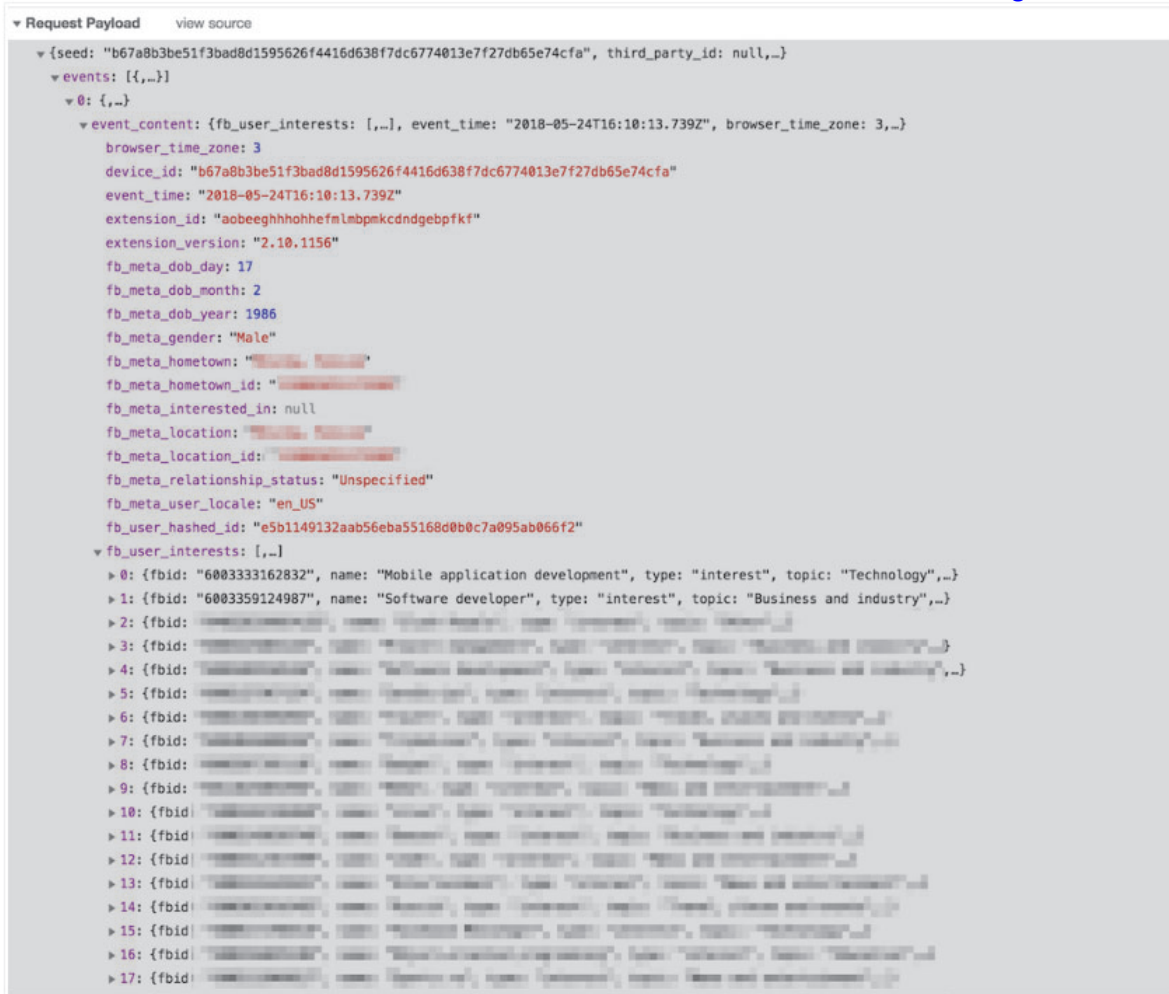
The inscrutable ways of your Facebook data

If you are logged into Facebook, these spyware extensions will scrape all your data immediately after the browser startup:



They even try to parse your purchase history! This alone is enough for these extensions to be booted from the Chrome Web Store.

All this data is then collected and sent to the `um-public-panel-prod.s3.amazonaws.com` domain, which is a named Amazon S3 instance rented by the spyware authors.



An alarming amount of data was being sent over to that server including all the Facebook "interests". In order to test this, I had to use my own account, so you can observe a piece of my own data, which I don't mind sharing with you.

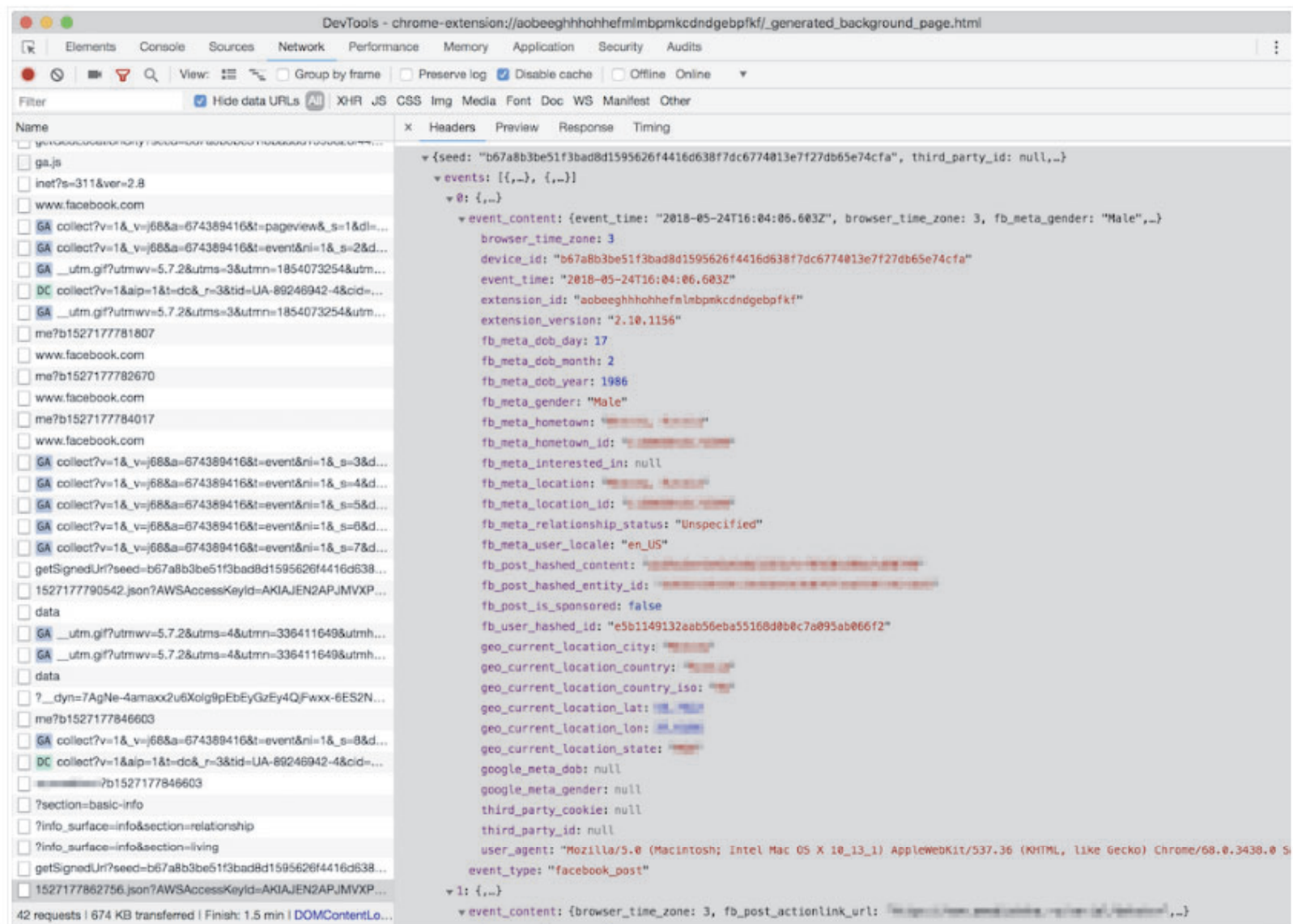
As you can see on the screenshot, they do not send a plain FB identifier; instead, they send it in a hashed form. I imagine that they think that this practice allow the spyware group to say that this data has been made "anonymous."

“Dear spyware developers, come on! Do you really believe that hashing a numeric value with a static salt cannot be decoded?”

```
SHA1("sME9Azj8G28Y" + userId) = e5b1149132aab56eba55168d0b0c7a095ab066f2
```

By the way, dear reader, here is a contest for you: the first one to crack the hash and discover my FB ID gets a free AdGuard license. Write your answer in the comments. No cheating, please :)

But hey, what is the good of having this data without the spyware company also knowing what exactly you do on the Internet? Wouldn't it be so much better if they knew what exact posts you read or what exact ads you see? Well, no worries, that's exactly what they do: they siphon information about all of the posts, sponsored posts, tweets, the YouTube videos and ads you see or interact with, along with a poorly hashed user ID and totally UN-hashed location data.



Meet Unimania Inc.

Who is behind this activity? The only thing I knew about the authors was the link to their extensions' privacy policy: http://privacy.unimania.xyz/privacy_policy.pdf (here's a [copy](#), just in case). As usual, there's a lot of confusing legalese about how you provide them with consent without doing anything, how seriously they care about your privacy, how strongly your data is made (or kept) anonymous and how it can in no way can be traced back to you as it is protected by a powerful mathematical "hash function."

Fortunately, it is also pretty transparent about what exact information about you is collected:

What Information We Collect and How We Collect It. In general, the Information we collect includes nonpersonally identifiable demographic and psychographic data as well as sponsored campaigns, advertisements or posts that target you directly or that have been shared with you.

Also, I found their [EULA \(copy\)](#) from which I learned that the company name is "Unimania, Inc." and they claim to be located in Tel-Aviv, Israel. However, I could not find any information on this company in the Israeli company register.

My story might have ended here, but there was a sentence in the privacy policy that caught my attention:

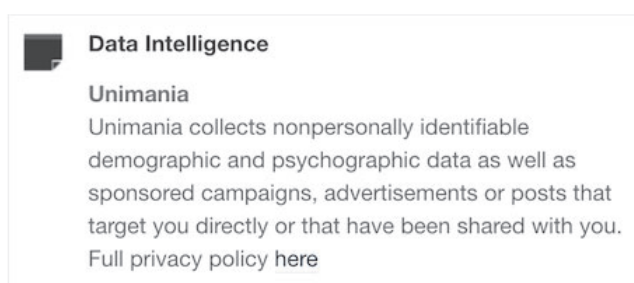
Background. You have been directed to this Privacy Policy from a separate and independent third party Google Chrome Extension or Mobile Software Application ("Third Party Software").

Mobile Software Application

"Mobile Software Application!" I said to myself.

So this was not just a matter limited to Chrome extensions, and I realized that I needed to continue my investigation. To this end, some good news was that we already had some data collected while preparing a [study on mobile apps tracking](#) and I could make use of it and query it right away.

That's how I found one particular app that was connecting to the Unimania servers. This was an alternative Facebook client called "[Fast - Social App](#)" with a record of more than 10,000,000 installs according to Google Play. The app developer does not bother to hide that fact and mentions Unimania in the privacy policy:



Scanning this developer apps' traffic confirmed that "Fast-Social App" transfers pretty much the same data as the Chrome extensions do, and to the same Unimania servers. I also found out that "[Fast Lite - Social App + Twitter](#)" (1,000,000+ installs) also does the same thing.

Besides that, I found a couple more apps that mention Unimania in their privacy policies. I cannot confirm that they are still leaking user data, but I can assume they were doing so in the past; otherwise, why would they mention it?

- [PhotoMania - Photo Effects](#) (1,000,000+ installs, [policy](#)).
- [All In One Social Media "Fast"](#) (100,000+ installs, [policy](#))

11. Third Party Software/Service

While using the Service we may be using third party software and/or service, in order to collect and/or process the information detailed herein. Such software includes without limitation, Google Analytics, which privacy policy is available at <http://www.google.com/intl/en/analytics/privacyoverview.html>, Amazon S3, which Privacy Policy is available at <http://aws.amazon.com/privacy.html>, and Unimania, which collects nonpersonally identifiable demographic and psychographic data as well as sponsored campaigns, advertisements or posts. Unimania's privacy policy is available at http://privacy.unimania.xyz/privacy_policy.pdf.

Finally, it seems that Unimania is about to launch their own "products":

- **OmniSocial** - a mobile app
- **Who's following me?** - a browser extension

Obviously, none of these apps describe this behavior in the app description; neither do they have an "in-app disclosure" as **required** by Google. I must admit that the Google Play Developer Policies look solid, and so they are likely not the reason of why the privacy of Android apps is in such a sad state. The problem is that these policies are **not enforced**, hence most of the app developers simply ignore them.

Summary

Congratulations for reading through such a long article (or for skipping all the boring technical details and jumping straight to the summary)!

Let's summarize what we discovered.

1. A huge spyware campaign engaging some Mobile Apps and Chrome extensions in stealing users' Facebook data and spying on their social network browsing history. The list of the information collected by these apps and extensions includes the user's Facebook profile data including demographics and the list of user interests. Also, they were collecting the users' browsing history including all the Facebook regular and sponsored posts, tweets, YouTube videos and ads.
2. Four spyware Chrome extensions with aggregated users count of more than 400,000 users.
3. Two Android apps with total installs count of more than 11,000,000 selling out their users data.
4. The campaign is run by a supposed Israeli company named "Unimania, Inc." Unfortunately, I was not able to trace this further back to Unimania's owners or affiliates and I can't say who is profiting from the data.

I've reported all the discovered apps and extensions to Google and I hope they take corrective measures soon.

How to protect yourself?

The answer to this question is both very simple and very difficult.

When installing anything on your device or browser, follow these rules:

- Read the privacy policy. It is not useless - everything discovered in this case was mentioned in the privacy policies.
- **Never ever install anything made by a developer you don't trust.** Do your homework, find out who the developer is and decide for yourself if they are trustworthy.

Also, all Unimania domains have now been **added** to the "AdGuard Spyware filter" and will be blocked automatically if you have it enabled in any of our **AdGuard products**, or if you use **AdGuard DNS**. Unfortunately, there is a browser limitation that prevents an extension from controlling requests made by other extensions so using the AdGuard Chrome extension or uBlock Origin may not be enough, even if you have the "AdGuard Spyware filter" enabled.

Alternatively, you can block these three domains by **adding** them to the "hosts" file:

- `um-public-panel-prod.s3.amazonaws.com`
- `collection-endpoint-prod.herokuapp.com`
- `collection-endpoint-staging.herokuapp.com`

UPD (Jun 3): The Android apps mentioned in the article are no more available on Google Play.

UPD (Jun 5): The Chrome extensions are finally taken down from the Chrome Web Store.

Andrey Meshkov on [AdGuard Research](#), [Industry News](#)

MAY 30, 2018

EXHIBIT 2

Home > Extensions > UpVoice



UpVoice

Offered by: UpVoice Team

★★★★★ 0 | Social & Communication

Available on Chrome

Overview

Reviews

Related



Overview

This extension allows you to earn rewards just for being you!

Win up to \$75 US in the first year for using our participating sites like you normally do. Share your opinions and win even more! Our participating sites are Facebook, YouTube, Twitter, Amazon, and LinkedIn.

As a qualified UpVoice panelist, you impact the marketing decisions and brand strategies of multi-billion dollars corporations, who compete for your attention online. This means that you have a direct influence on the online advertising campaigns of big brands.

Install the UpVoice extension and qualify to become a member of our panel. It's safe and won't impact your browser performance. As a qualified member, we will reward you for browsing your social feeds and other participating sites normally. For more details, please visit our terms of service at: <https://joinupvoice.com/tos>.

Make sure to disable your ad blocker, if you have one, otherwise, we cannot collect the ads that target you and therefore we cannot reward you.

Privacy & data collection

When you regularly visit Facebook, Instagram and other participating sites, we securely collect the ads that you see and anonymous demographic profile data. We never share your personal information with anyone, except if needed to send you your rewards.

We protect your data using the highest security standards and we comply with all privacy regulations. For more details, please visit our Privacy Policy at: <https://joinupvoice.com/privacy> and our Data & Privacy FAQ at: <https://www.joinupvoice.com/faq>

If you have any questions, please contact us at: contact@joinupvoice.com. For more details please visit www.joinupvoice.com.

[Read less](#)

Additional Information

[Website](#) [Report abuse](#)

Version
2.10.1445

Updated
October 12, 2020

Size
358KiB

Language
English

Developer
[Contact the developer](#)
[Privacy Policy](#)

This extension allows you to earn rewards just for being you!

Available on Chrome

EXHIBIT 3

Home > Extensions > UpVoice

UpVoice

Offered by: UpVoice Team

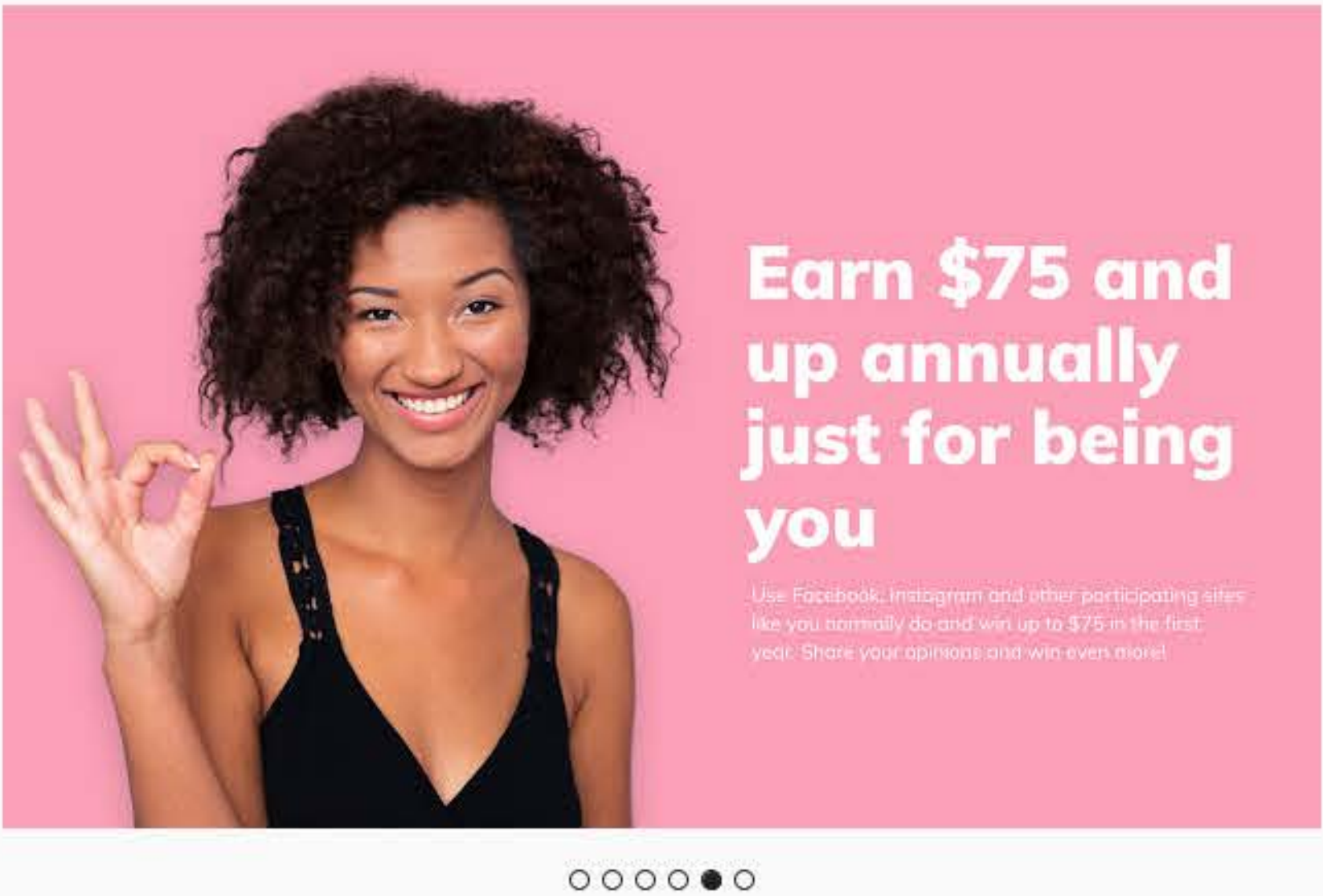
★★★★★ 0 | Social & Communication | 30 users

Available on Chrome

Overview

Reviews

Related



Overview

This extension allows you to earn rewards just for being you!

Get rewarded for visiting our participating sites (Facebook, YouTube, Twitter, Amazon, and LinkedIn) like you normally do! You'll get a \$5 signup reward immediately!

As a qualified UpVoice panelist, you impact the marketing decisions and brand strategies of multi-billion dollars corporations who compete for your attention online. This means that you have a direct influence on the online advertising campaigns of big brands.

Install the UpVoice extension and qualify to become a member of our panel. It's safe and won't impact your browser performance. As a qualified member, we will reward you for browsing your social feeds and other participating sites regularly. For more details, please visit our terms of service at: <https://joinupvoice.com/tos>.

Make sure to disable your ad blocker, if you have one. Otherwise, we cannot collect the ads that target you and therefore we cannot reward you.

Privacy & data collection

When you regularly visit our participating sites, we securely collect the ads that you see and anonymous demographic profile data. We never share your personal information with anyone, except if needed to send you your rewards. We protect your data using the highest security standards and we comply with all privacy regulations. For more details, please visit our Privacy Policy at: <https://joinupvoice.com/privacy> and our Data & Privacy FAQ at: <https://www.joinupvoice.com/faq>

If you have any questions, please contact us at: contact@joinupvoice.com. For more details please visit www.joinupvoice.com

Read less

Additional Information

[Website](#) [Report abuse](#)

Version
2.10.1445

Updated
October 14, 2020

Size
358KiB

Language
English

Developer
[Contact the developer](#)
[Privacy Policy](#)

This extension allows you to earn rewards just for being you!

Available on Chrome

EXHIBIT 18

REDACTED VERSION OF
EXHIBIT FILED UNDER
SEAL

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

META PLATFORMS, INC., a
Delaware corporation,

Plaintiffs,

v.

BRANDTOTAL LTD., an Israeli
corporation, and UNIMANIA, INC.,
a Delaware corporation,

Defendants.

Civil Action No.: 3:20-CV-07182-JCS

Chief Magistrate Judge Joseph C. Spero

OPENING EXPERT REPORT OF DAVID MARTENS
JANUARY 12, 2022

TABLE OF CONTENTS

PART I. INTRODUCTION AND SUMMARY OF OPINIONS.....	10
1 Assignment.....	10
2 Qualifications.....	10
2.1 Employment Experience	11
2.2 Software Experience	11
2.3 Education	13
2.4 General Professional Experience.....	13
2.5 Summary Of Experience And Qualifications.....	14
3 Summary of Findings	15
3.1 Overview	15
3.2 Opinions	17
3.3 Summary Chart	24
PART II. BACKGROUND	27
4 Background	27
4.1 Facebook Overview.....	27
4.2 Facebook Account Creation.....	29
4.3 Instagram Overview	32
4.4 Instagram Account Creation	33
4.5 Facebook and Instagram Rules	36
4.6 BrandTotal.....	41
4.7 BrandTotal’s Collection Methods	42

4.7.1	Active Collection	42
4.7.2	Reactive Collection.....	43
4.7.3	Direct Collection.....	45
4.8	Access Mechanisms.....	45
4.8.1	Username And Password	46
4.8.2	Access Tokens.....	47
4.8.3	Cookies	49
4.8.4	The Need To Protect Access Credentials	51
4.8.5	Anonymous Cookies.....	52
4.9	Use Of Access Credentials With Facebook And Instagram.....	53
4.9.1	Facebook	53
4.9.2	Instagram.....	57
4.9.3	Facebook and Instagram’s Graph API.....	61
4.10	Types Of Data Collected By BrandTotal.....	63
4.10.1	Access Tokens and Cookies.....	63
4.10.2	User Sign Up Data.....	63
4.10.3	User Technical Data.....	63
4.10.4	Demographic Data	64
4.10.5	Location Data	64
4.10.6	User Interests.....	64
4.10.7	Sponsored Posts Data	65
4.10.8	Non-Sponsored Posts Data	65
4.10.9	User Interaction Data	65
4.10.10	Advertising Interaction Data.....	65

4.10.11	Instagram-specific Data	66
4.11	BrandTotal’s Technical Architecture	66
4.12	Third Party Services Used By BrandTotal.....	68
4.12.1	Rapid7	68
4.12.2	Heroku	69
4.12.3	Amazon Web Services (AWS).....	70
4.12.4	Amazon S3 Database	70
4.12.5	Amazon Lambda Functions.....	71
4.12.6	Amazon Simple Queue Service (SQS).....	73
4.12.7	Amazon Relational Database Service (RDS).....	73
4.12.8	CloudFront CDN.....	74
4.13	Password-Protected v. Non-Password-Protected Areas.....	75
4.13.1	Password-Protected Area	75
4.13.2	Non-Password Protected Areas	76
4.13.3	Graph API Restricts Data That Can Be Obtained Without Access Credentials.....	76
4.13.4	Meta Uses Lockout Mechanisms To Restrict Access.....	82
4.13.5	Restricted Content is Always Password-protected Content	87
4.14	Notable Features Of BrandTotal’s Technology	93
4.14.1	Dynamically Downloaded Source Code	93
4.14.2	Manipulation Of User-agent Header	96
4.14.3	Use Of Proxies	96
4.14.4	Use Of Fake Accounts.....	98
4.14.5	The Shared Computer Problem	99

4.14.6 In-Application Browsers	100
4.14.7 Use Of Weak Hashing.....	102
4.14.8 Transmission And Storage Of Unencrypted Information	104
4.14.9 Lack Of Forced Update Mechanisms.....	105
4.14.10 Installed Base	107
4.14.11 Common Software Framework.....	107
4.15 Analytical Methods	108
4.15.1 Source Code Review	108
4.15.2 BrandTotal Technical Documentation.....	109
4.15.3 Network Tracing	110
4.15.4 Database Review	110
4.15.5 Rapid7 Logfile Review.....	111
4.15.6 APKPure.....	111
4.15.7 Sideloadng.....	111
4.15.8 Review Of Case Documents	112
4.16 Obstacles To Analysis	113
4.16.1 Source Code Production Deficiencies.....	113
4.16.2 Rapid7 Log Deletion	113
4.16.3 Late Produced Technical Documentation	114
4.16.4 Absence Of Knowledgeable Technical Witnesses	115
PART III. ANALYSIS.....	115
5 Amount of Data Obtained by BrandTotal.....	115
5.1 Data Obtained By Type.....	116

5.2	Data Obtained By Extension.....	117
6	BrandTotal's Server-Side Collection Code	120
6.1	Overview	120
6.2	Type Of Data Obtained	121
6.3	Amount Of Data Obtained.....	121
6.4	Collection Mechanism Used.....	121
6.4.1	FBEngagementsFetcherWorker Lambda Function	123
6.4.2	Other Lambda Functions.....	130
6.4.3	Use of Specific Access Tokens.....	132
6.5	Dates Of Operation	138
6.6	Other Notable Features	138
6.6.1	Scalability.....	138
6.6.2	Use Of Proxy.....	139
6.6.3	Header Manipulation.....	140
6.6.4	BrandTotal Awareness Of Overuse Risk.....	141
7	BrandTotal's Instagram-Targeting Applications	143
7.1	Overview	143
7.2	Summary Of Findings	144
7.3	Collection Mechanism Used.....	145
7.3.1	ASV And SSB Perform Active Collection	145
7.3.2	ASV And SSB Perform Reactive Collection.....	148
7.4	Collection From Password-Protected Areas	148
7.5	Types Of Data Obtained.....	150
7.5.1	Network Tracing	151

7.6	Dates Of Operation	162
7.6.1	Data Analysis.....	162
7.6.2	Rapid7 Analysis.....	163
7.7	Other Notable Features	164
7.7.1	ASV/SSB Misrepresents Itself	164
7.7.2	Addition Of Logger Function To BrandTotal Source Code	166
7.7.3	Use Of APKPure	168
7.7.4	Transmission Of Tokens Without Encryption	168
7.8	User-Facing Functionality.....	169
8	UpVoice 2021 Browser Extensions And Windows Application.....	172
8.1	Overview	172
8.2	Summary Of Findings	173
8.3	Collection Mechanism Used	174
8.3.1	UpVoice 2021 Engages In Reactive Collection.....	174
8.4	Collection From Password-Protected Areas	176
8.5	Types Of Data Obtained.....	176
8.6	Dates Of Operation	181
8.7	Other Notable Features	181
8.7.1	Use Of Dynamically Downloaded Code	181
8.7.2	Use Of A Hashed Facebook Identifier	181
8.7.3	Common Software Framework	183
8.7.4	Dynamic Downloading of Source Code.....	183
8.8	User Experience	184
8.8.1	Sign Up And Account Creation	184

9	UpVoice 2019 And Related Browser Extensions	190
9.1	Overview	190
9.2	Summary Of Findings	191
9.3	Collection Mechanism Used	192
9.3.1	Active Collection	192
9.3.2	Reactive Collection.....	194
9.4	Collection From Password-Protected Areas	195
9.5	Types Of Data Obtained.....	195
9.6	Dates Of Operation	196
9.7	Other Notable Features	198
9.7.1	Use Of Static Salt Hashing Function.....	198
9.7.2	UpVoice 2019 Is Susceptible To The Shared Computer Problem....	200
9.7.3	Common Software Framework	200
9.7.4	Dynamic Downloading of Source Code.....	201
10	BrandTotal's Facebook-Targeting Applications (Phoenix and Social One)	202
10.1	Overview	202
10.2	Summary Of Findings	203
10.3	Collection Mechanisms Used	204
10.3.1	Active Collection By Early Phoenix/Social One.....	205
10.3.2	Reactive Collection By Phoenix/Social One.....	208
10.4	Collection From Password-Protected Areas	212
10.5	Types Of Data Obtained.....	213
10.6	Dates Of Operation	214
10.7	Other Notable Features	214

	10.7.1 Dynamically Downloaded Code.....	214
	10.7.2 Social One Misrepresents Itself to Facebook’s Servers.....	218
	10.7.3 No Forced Update Mechanism	221
	10.8 User Experience	222
	10.8.1 Social One	222
	10.8.2 Phoenix.....	224
11	Restricted Panel Software	225
	11.1 Restricted Panel Lambda Function.....	226
	11.2 Restricted Panel Browser Extension	227
	11.3 Rapid7 Logs Show BrandTotal Accessing Restricted Content.....	228
	11.4 Restricted Panel Data In MySQL.....	230
12	Non-Collection Extensions	231
13	Conclusion	232

PART I. INTRODUCTION AND SUMMARY OF OPINIONS

1 Assignment

1. I, David Martens, have been retained by Meta Platforms, Inc. (“Meta”) through the law firm of WILMER CUTLER PICKERING HALE AND DORR, LLP as an expert witness in the matter of Meta Platforms Inc. v. BrandTotal, Ltd. and Unimania, Inc., Civil Action No. 3:20-cv-07182 (hereinafter “the present matter”). For purposes of this report, I will refer to BrandTotal, Ltd. and Unimania, Inc. collectively as “BrandTotal.”

2. My compensation is \$275 per hour for testimonial and non-testimonial time. My compensation is not affected in any way by the opinions I offer, the conclusions I reach, or the outcome of the present matter.

3. I have not previously submitted an expert report in the present matter. I submit this opening report on the issue of technical aspects of BrandTotal’s applications, browser extensions, and server-side collection software as well as BrandTotal’s use of that technology in ways that meet the elements of the legal claims Facebook has asserted against BrandTotal.

2 Qualifications

4. I have extensive experience in the technologies at issue in the present matter. I am prepared to testify regarding my qualifications, background and experience relevant to the issues in this matter. A copy of my Curriculum Vitae, including prior testimonial experience, is attached as Appendix A.

2.1 Employment Experience

5. I run my own consulting business (Intuity Consultants) and my own law firm (Intuity, PC). My consulting business and law firm concern intellectual property matters. I have been in technology consulting for more than five years, I litigated technology cases at other law firms for seven years prior to starting my own firms, clerked at law firms working on technology cases during law school, and I was an engineer at Intel, IBM microelectronics, and Sun Microsystems for fourteen years prior. I have been employed in these capacities since 1990.

2.2 Software Experience

6. I have written source code extensively in many languages including C, C++, several versions of assembly, Python, Perl, Fortran, BASIC, Java, SQL, Verilog, VHDL and a number of languages that were specific to jobs I held in technology. I am also familiar with several languages for which I have reviewed source code or written only smaller projects, such as C#, Visual Basic, JavaScript, TypeScript, Ruby, Objective C, and other versions of assembly.

7. I am familiar with the practice of data scraping. I have written several web scrapers in response to client requests. In one example, Toshiba needed to collect user manuals and other technical documents from Toshiba's customer support website to meet document collection requirements in a television-related litigation in which Toshiba was a defendant. Toshiba could not collect these documents in a time frame that was consistent with Toshiba's discovery obligations, so the law firm partner I worked with asked me if I could write a web scraper to collect those documents. In response, I wrote a web scraper

in Python that collected all of Toshiba's user manuals and content from Toshiba's user support forums to meet Toshiba's discovery obligations.

8. In another example, Comcast needed to collect information from its internal design wiki (Confluence), in response to discovery requests for a litigation involving Comcast's set-top boxes. Comcast had a third-party vendor that attempted to gather content from Comcast's Confluence site, but that vendor had issues collecting some portions of the Confluence site, so I was asked to write a web scraper to collect Comcast's Confluence content. In response, I wrote a web scraper in Python that collected the relevant portion of Comcast's Confluence site to meet Comcast's discovery obligations.

9. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

10. BrandTotal's Android applications are written in Java. I have been writing Java since 1996. Java is a very common language for server-side and Android application development, so I frequently interpret Java source code in the ordinary course of my work for clients. Thus, I have substantial familiarity with Java code at issue in the present matter.

11. BrandTotal's browser extensions are written in TypeScript (a variation of JavaScript). I have been writing JavaScript since 2005. JavaScript is a very common language for browser-based software development. I frequently interpret JavaScript in the

ordinary course of my work for clients. Thus, I have substantial familiarity with [REDACTED]

12. I also have considerable experience with source code control systems such as Git. BrandTotal's source code production included Git repositories. My familiarity with Git allowed me to extract different versions of source code, and associated metadata, from BrandTotal's Git repositories.

2.3 Education

13. I received a Bachelor's degree in Electrical Engineering from the University of Wisconsin Platteville in 1990 and a Master's degree in Electrical Engineering from Stanford University in 1998. My focus during my graduate studies was on computer architecture, software, and computer circuits.

2.4 General Professional Experience

14. I was a practicing engineer for fourteen years. I designed integrated circuits, and wrote software to support designing integrated circuits, at Intel, IBM, and Sun Microsystems. Most of my design activities were on next-generation microprocessors, which involves a tight coupling of hardware and software principles. I was awarded six patents for innovations during my engineering career.

15. After leaving Sun Microsystems, I went to law school to pursue an interest in patent litigation. I worked at several firms during law school, and I joined the Finnegan Henderson firm as a clerk during my last year of law school and worked with them for five years. I followed a mentor of mine to Winston & Strawn in 2013 and formed my own firms in 2016.

16. During my time at these firms, I spent a majority of my time on litigations involving software source code. More specifically, I typically took on a hybrid role that was one-part technical expert and another part attorney. In this hybrid role, I have deposed more than twenty engineers, including many Apple iOS software engineers, on specific aspects of their source code. I have also cross-examined at trial one of Apple's most senior designers on detailed technical aspects of Apple's next-generation iPhone. I formed my own firms so I could focus on the most interesting aspect of intellectual property litigations – resolving difficult technical issues in ways that businesspeople and courts could use to resolve larger questions.

17. I develop software in the ordinary course of my consulting work. Some clients have technical needs that require advanced data analysis or automated data retrieval. I spend several hundred hours per year developing software to support my consulting clients.

18. I am also a very active programmer in my free time. I spend several hundred hours per year, beyond the requirements of my client engagements, developing Python source code for personal interest projects including projects for a non-profit museum for which I have been a Director since 1999.

2.5 Summary Of Experience And Qualifications

19. By virtue of my extended professional and educational experience, as summarized above, I have gained a detailed understanding of computer software including issues implicated in the present matter. All the issues I have faced in this engagement were

either directly within my prior experience or were minor extrapolations from similar issues I faced in other professional contexts.

3 Summary of Findings

3.1 Overview

20. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

21. [REDACTED]

[REDACTED]

[REDACTED]

22. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

23. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

24. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

25. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

¹ BT0005496

26. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]²

27. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

3.2 Opinions

28. [REDACTED]

[REDACTED]

[REDACTED]^{3,4}

29. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

² BT0005482

³ [REDACTED]

⁴ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- Facebook-Targeting Applications (Social One and Phoenix)
- Instagram-Targeting Applications (Anonymous Story Viewer for Instagram and Story Savebox).

34. “Reactive Collection” involves automated collection of data from Facebook or Instagram through software that engages in constant surveillance of the activities of an authenticated user while they browse and interact with Password-Protected Areas of Facebook or Instagram and extracts data based on those interactions.⁷

35. It is my opinion that the following BrandTotal applications and extensions engage in Reactive Collection from Password-Protected Areas of Facebook and Instagram:⁸

- UpVoice 2021 (including the Chrome Extension, Edge Extension, and Windows Application versions).
- UpVoice 2019 and related browser extensions (Ads Feed, Who’s Following Me, and Social Video Downloader).
- Facebook-Targeting Applications (Social One and Phoenix)
- Instagram-Targeting Applications (Anonymous Story Viewer and Story Savebox).

⁷ See Background Section for a full definition and explanation of the term “Reactive Collection.”

⁸ The dates during which each application and extension engaged in Reactive Collection are equivalent to the dates listed in the “Dates of Operation” column of the chart below in Section 3.3 as discussed in more detail in Sections 7, 8, 9, and 10 below.

■ [REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED] [REDACTED] [REDACTED]

- | [REDACTED]
- | [REDACTED]
- | [REDACTED]
- | [REDACTED]
- | [REDACTED]
- [REDACTED]
- | [REDACTED]
- | [REDACTED]
- [REDACTED]
- | [REDACTED]
- [REDACTED]
- | [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

■ [REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

3.3 Summary Chart

51. BrandTotal employs at least fourteen Data Collection mechanisms.¹⁴ Each is discussed in more detail in the body of this report. The following chart provides an overview of my findings.

[REDACTED]					
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

¹⁴ My analysis identified additional mechanisms not disclosed by BrandTotal during discovery. My findings on these mechanisms are preliminary and not included in this chart but are described in § 11 below.

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

				<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>
<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> <div></div> <div></div> </div>	
<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> <div></div> <div></div> </div>	<div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> </div>
<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> <div></div> <div></div> </div>	<div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> </div>
<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>
<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> <div></div> <div></div> </div>	<div> <div></div> <div></div> <div></div> <div></div> </div>

				[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

PART II. BACKGROUND

- 1 [REDACTED]
- 2 [REDACTED]
- 3 [REDACTED]
- 4 [REDACTED]
- 5 [REDACTED]

[REDACTED]

18 [REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

²⁵ The following description and screenshots of Instagram's functionality and user interface were current as of November 2021.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

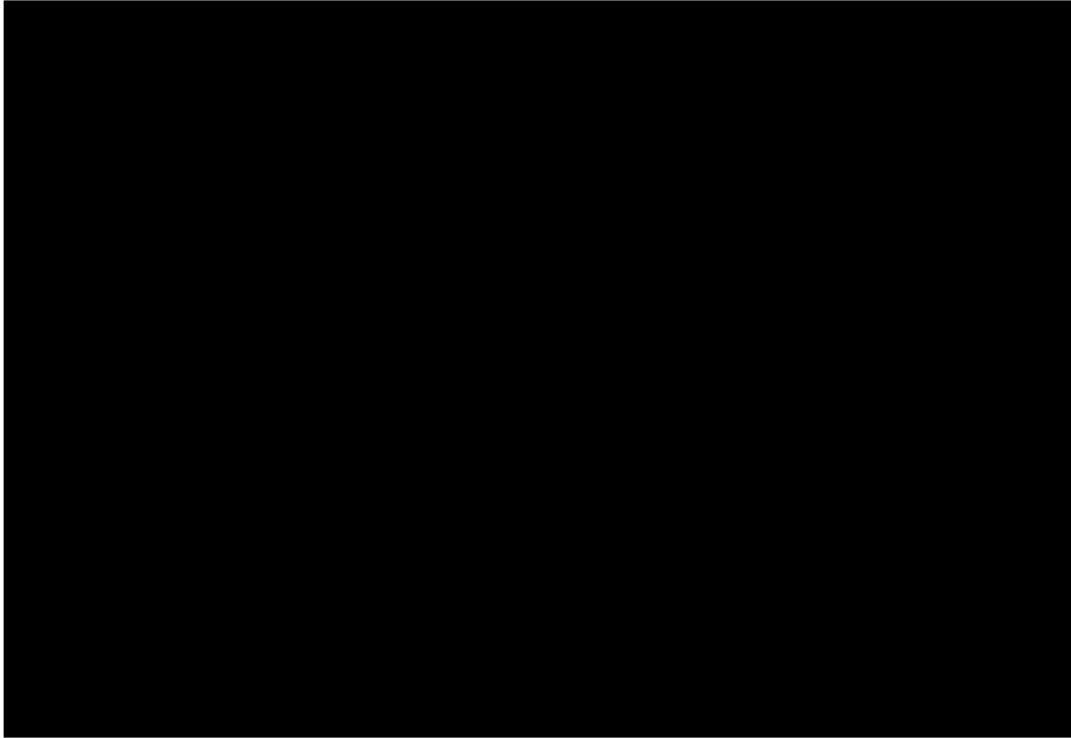
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]



■ [REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

[REDACTED]

³² See Facebook's Terms of Service, Section 3.1, available at <https://www.facebook.com/terms.php> (last visited December 3, 2021).

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

■ [REDACTED]

[REDACTED]

See <https://help.instagram.com/581066165581870>.

94.

[REDACTED]

³⁶ See Instagram's Terms of Use, available at <https://help.instagram.com/581066165581870> (last visited December 8, 2021).

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

99. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

37 [REDACTED]

38 [REDACTED]

[REDACTED]

[REDACTED]

100. In this way Active Collection can be thought of as a “trojan horse” form of data access and collection. BrandTotal technology that engages in Active Collection needs an authenticated user in order to obtain access to and get inside the walls of Password-Protected Areas of Facebook and Instagram. Once it has gained this access, software that engages in Active Collection no longer depends on any additional user inputs but generates its own requests to call for, obtain, and exfiltrate information.

101. An example of Active Collection is a BrandTotal application requesting and retrieving, for a logged-in Facebook user, demographic information about that user regardless of whether the user took any steps to access that information themselves.

102. Active Collection is automated Data Collection as it involves the accessing and obtaining of data from Facebook or Instagram through programmatic and technological means without manual human input.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

████████████████████

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

51 [REDACTED]
52 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

53 [REDACTED]

<p>  </p>	<p>  </p>
<p>  </p>	<p>  </p>

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

58 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

60 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

⁶¹ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

62 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

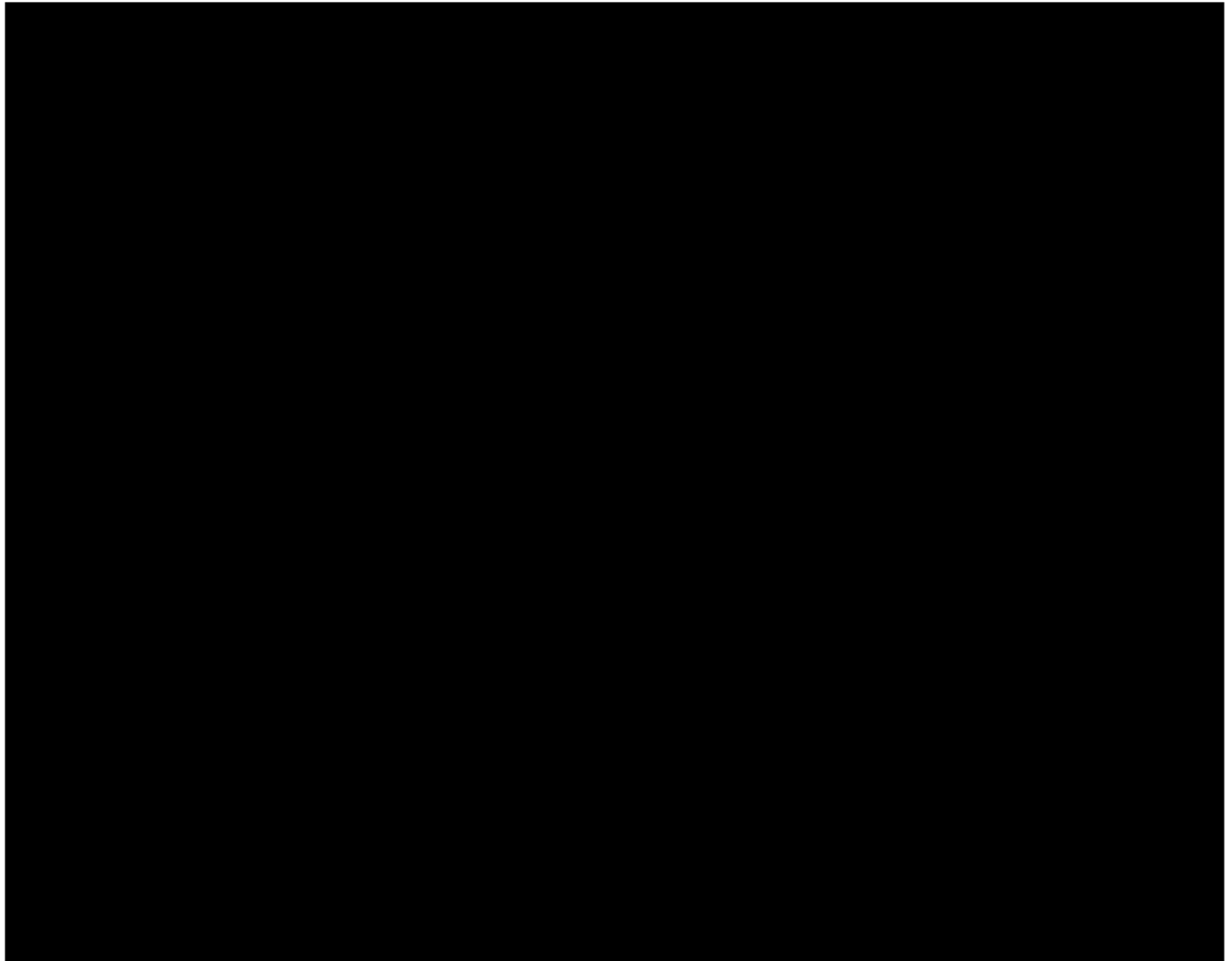
[REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

⁶⁸ BT0001889.



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

85 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

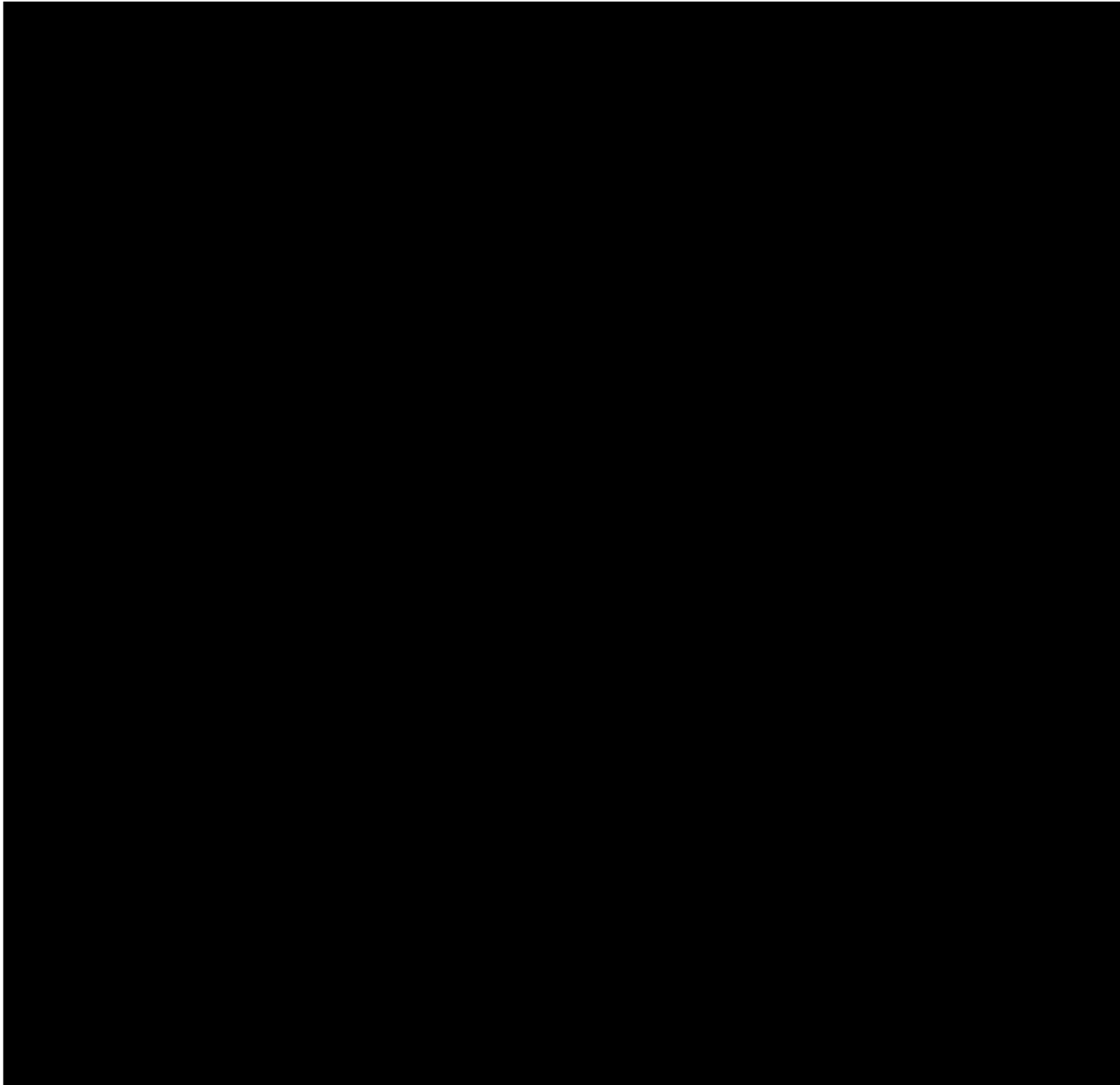
[REDACTED]

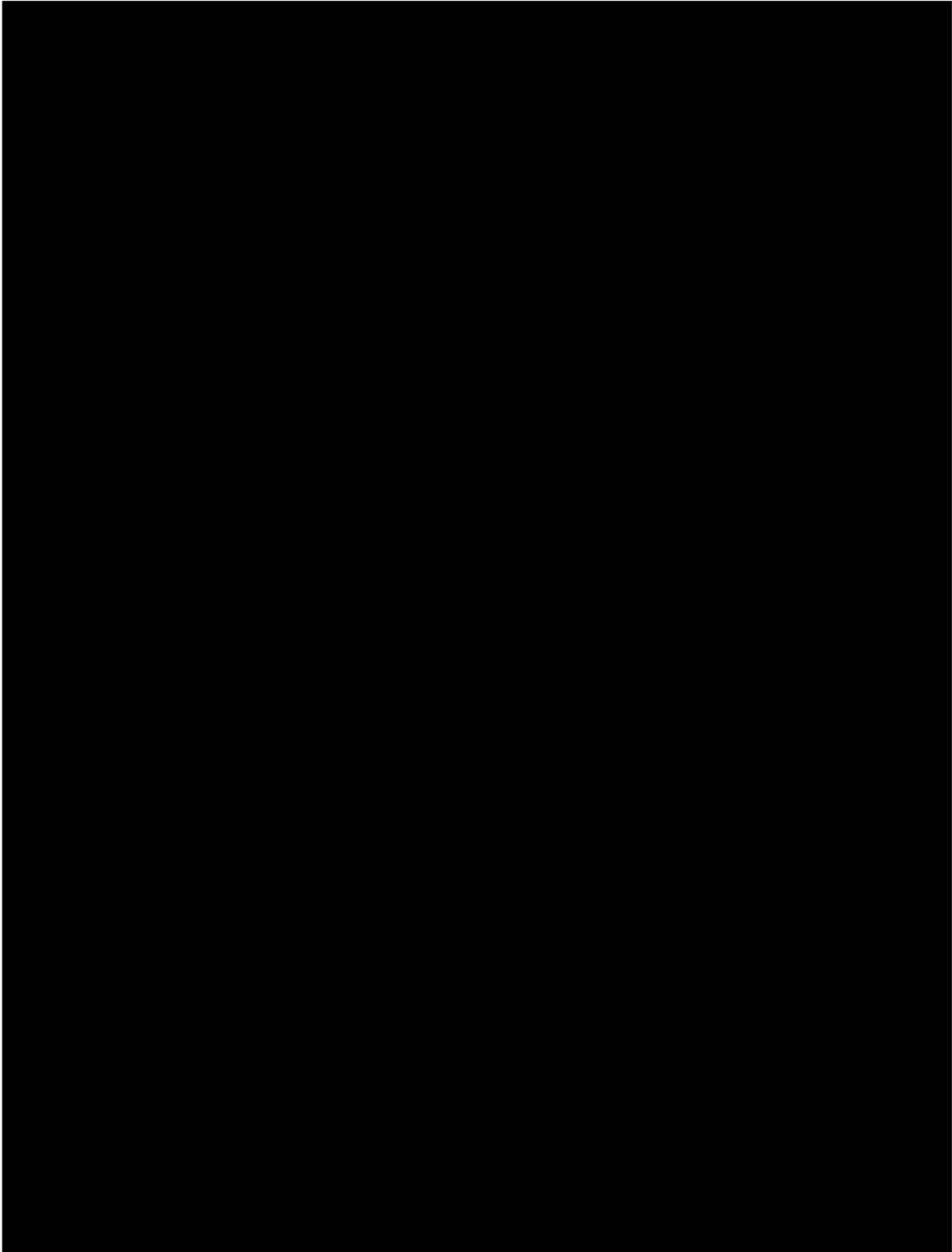
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]





[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

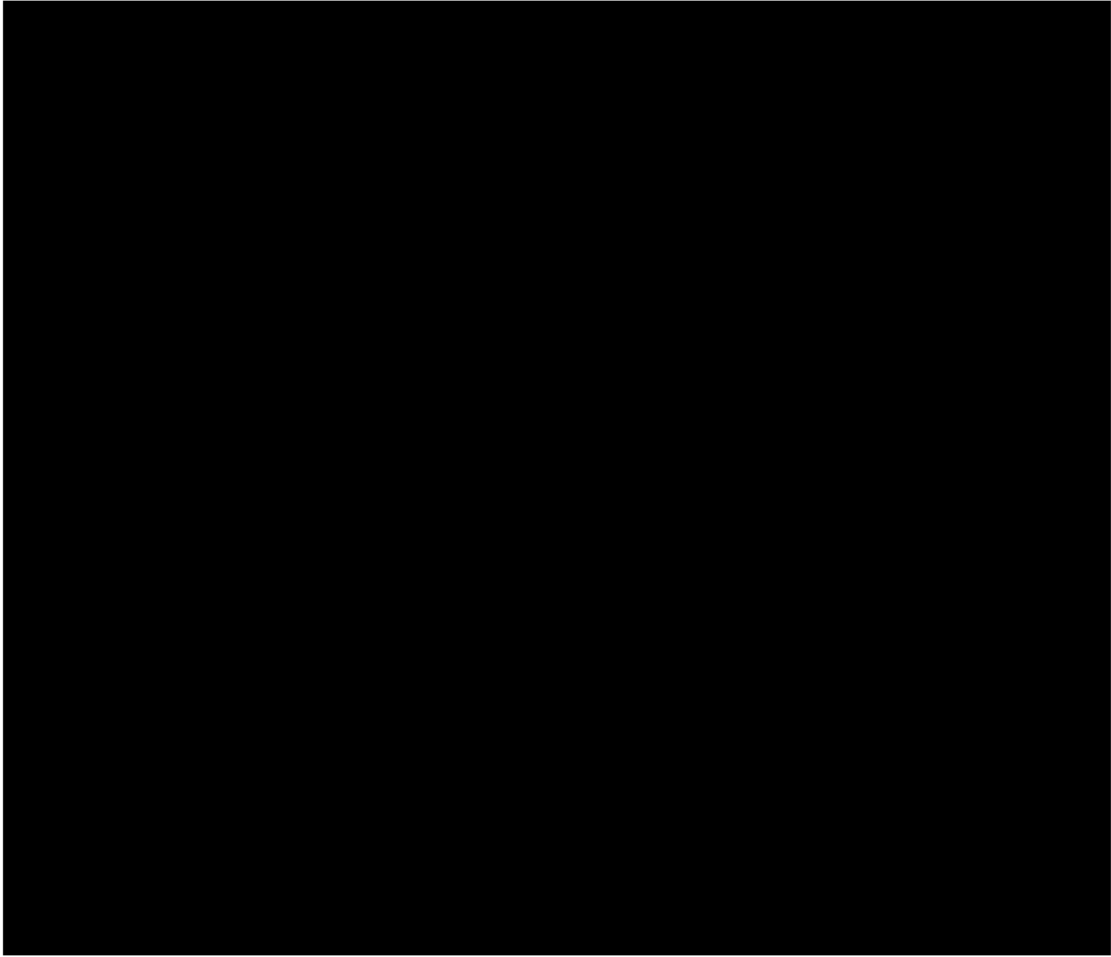
[REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

118 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The image is entirely black and contains no visible content.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

132 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
[REDACTED]
[REDACTED] BT0005490.

283. [REDACTED]
[REDACTED]

4.15.3 Network Tracing

284. “Network Tracing” is a process whereby a software application captures and stores network communications between a first computing device and a second computing device or computer-based service. “Fiddler” is one example of an application that performs Network Tracing.¹⁴⁸

285. Network Tracing results typically take the form of a file whose filename ends in “.saz.” These results contain most or all network communications between the devices involved, including the header and payload portions of the requests and responses for each communication. Network Tracing is a useful analytical technique for understanding the nature of, and contents of, network communications between two devices. My analyses includes Network Tracing results.

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

¹⁴⁸ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

Figure 1

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

I	[REDACTED]
---	------------

[REDACTED]
[REDACTED] [REDACTED]
[REDACTED]

[illegible]

■	[REDACTED]
■	[REDACTED]
■	[REDACTED]

■ [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

■ [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

■ [REDACTED]

The image consists of a single, uniform black rectangle covering the entire area. There are no discernible features, text, or patterns.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

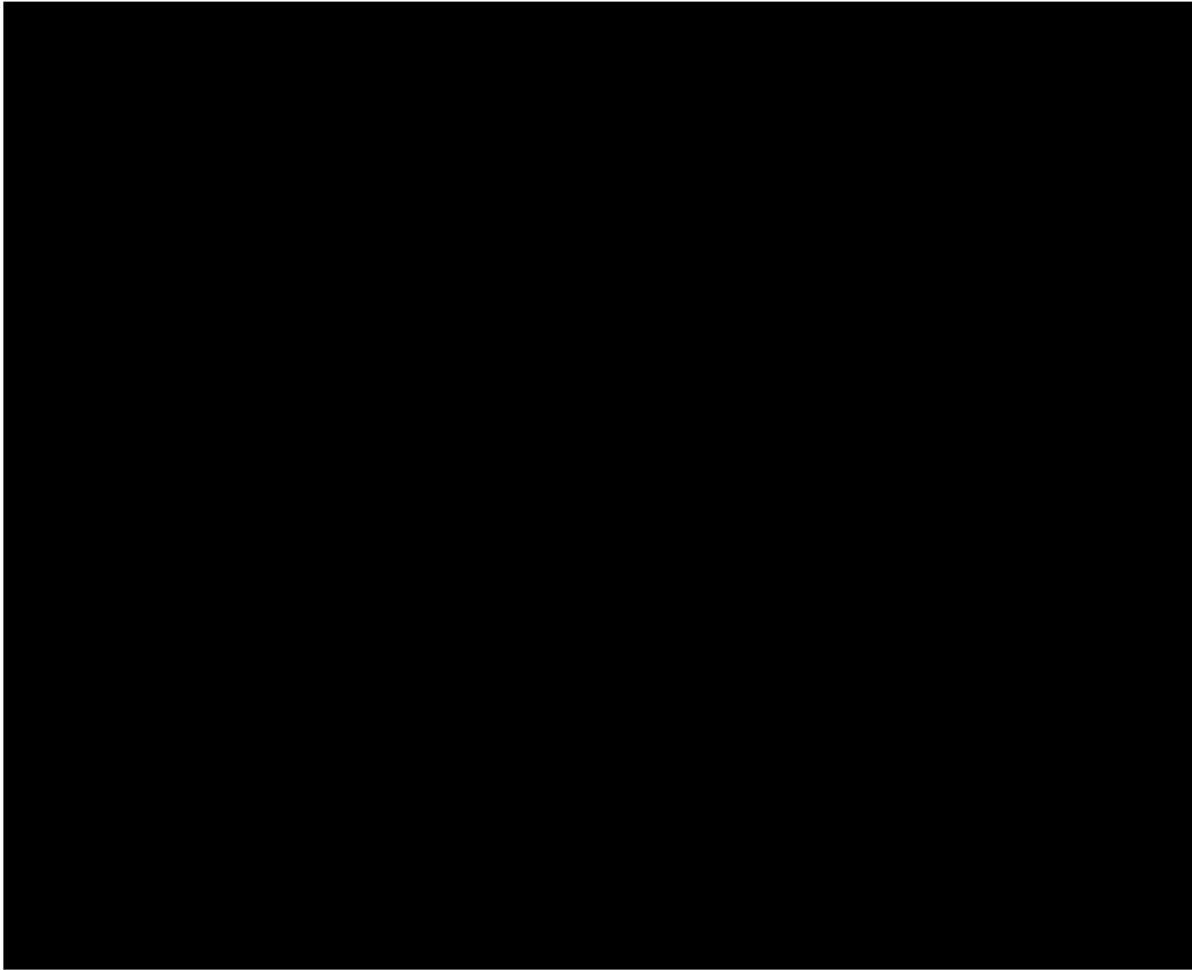
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible][illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

██████████

██████████

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

██████████

15 JULY 2004

the 1990s, the number of people in the United States who are 65 years of age or older has increased by 50 percent, and the number of people 75 years of age or older has increased by 75 percent. The number of people 85 years of age or older has increased by 150 percent. The number of people 95 years of age or older has increased by 300 percent. The number of people 100 years of age or older has increased by 500 percent. The number of people 105 years of age or older has increased by 1,000 percent. The number of people 110 years of age or older has increased by 2,000 percent. The number of people 115 years of age or older has increased by 4,000 percent. The number of people 120 years of age or older has increased by 8,000 percent. The number of people 125 years of age or older has increased by 16,000 percent. The number of people 130 years of age or older has increased by 32,000 percent. The number of people 135 years of age or older has increased by 64,000 percent. The number of people 140 years of age or older has increased by 128,000 percent. The number of people 145 years of age or older has increased by 256,000 percent. The number of people 150 years of age or older has increased by 512,000 percent. The number of people 155 years of age or older has increased by 1,024,000 percent. The number of people 160 years of age or older has increased by 2,048,000 percent. The number of people 165 years of age or older has increased by 4,096,000 percent. The number of people 170 years of age or older has increased by 8,192,000 percent. The number of people 175 years of age or older has increased by 16,384,000 percent. The number of people 180 years of age or older has increased by 32,768,000 percent. The number of people 185 years of age or older has increased by 65,536,000 percent. The number of people 190 years of age or older has increased by 131,072,000 percent. The number of people 195 years of age or older has increased by 262,144,000 percent. The number of people 200 years of age or older has increased by 524,288,000 percent. The number of people 205 years of age or older has increased by 1,048,576,000 percent. The number of people 210 years of age or older has increased by 2,097,152,000 percent. The number of people 215 years of age or older has increased by 4,194,304,000 percent. The number of people 220 years of age or older has increased by 8,388,608,000 percent. The number of people 225 years of age or older has increased by 16,777,216,000 percent. The number of people 230 years of age or older has increased by 33,554,432,000 percent. The number of people 235 years of age or older has increased by 67,108,864,000 percent. The number of people 240 years of age or older has increased by 134,217,728,000 percent. The number of people 245 years of age or older has increased by 268,435,456,000 percent. The number of people 250 years of age or older has increased by 536,870,912,000 percent. The number of people 255 years of age or older has increased by 1,073,741,824,000 percent. The number of people 260 years of age or older has increased by 2,147,483,648,000 percent. The number of people 265 years of age or older has increased by 4,294,967,296,000 percent. The number of people 270 years of age or older has increased by 8,589,934,592,000 percent. The number of people 275 years of age or older has increased by 17,179,869,184,000 percent. The number of people 280 years of age or older has increased by 34,359,738,368,000 percent. The number of people 285 years of age or older has increased by 68,719,476,736,000 percent. The number of people 290 years of age or older has increased by 137,438,953,472,000 percent. The number of people 295 years of age or older has increased by 274,877,906,944,000 percent. The number of people 300 years of age or older has increased by 549,755,813,888,000 percent. The number of people 305 years of age or older has increased by 1,099,511,627,776,000 percent. The number of people 310 years of age or older has increased by 2,199,023,255,552,000 percent. The number of people 315 years of age or older has increased by 4,398,046,511,104,000 percent. The number of people 320 years of age or older has increased by 8,796,093,022,208,000 percent. The number of people 325 years of age or older has increased by 17,592,186,044,416,000 percent. The number of people 330 years of age or older has increased by 35,184,372,088,832,000 percent. The number of people 335 years of age or older has increased by 70,368,744,177,664,000 percent. The number of people 340 years of age or older has increased by 140,737,488,355,328,000 percent. The number of people 345 years of age or older has increased by 281,474,976,710,656,000 percent. The number of people 350 years of age or older has increased by 562,949,953,421,312,000 percent. The number of people 355 years of age or older has increased by 1,125,899,906,842,624,000 percent. The number of people 360 years of age or older has increased by 2,251,799,813,685,248,000 percent. The number of people 365 years of age or older has increased by 4,503,599,627,370,496,000 percent. The number of people 370 years of age or older has increased by 9,007,199,254,740,992,000 percent. The number of people 375 years of age or older has increased by 18,014,398,509,481,984,000 percent. The number of people 380 years of age or older has increased by 36,028,797,018,963,968,000 percent. The number of people 385 years of age or older has increased by 72,057,594,037,927,936,000 percent. The number of people 390 years of age or older has increased by 144,115,188,075,855,872,000 percent. The number of people 395 years of age or older has increased by 288,230,376,151,711,744,000 percent. The number of people 400 years of age or older has increased by 576,460,752,303,423,488,000 percent. The number of people 405 years of age or older has increased by 1,152,921,504,606,846,976,000 percent. The number of people 410 years of age or older has increased by 2,305,843,009,213,693,952,000 percent. The number of people 415 years of age or older has increased by 4,611,686,018,427,387,904,000 percent. The number of people 420 years of age or older has increased by 9,223,372,036,854,775,808,000 percent. The number of people 425 years of age or older has increased by 18,446,744,073,709,551,616,000 percent. The number of people 430 years of age or older has increased by 36,893,488,147,419,103,232,000 percent. The number of people 435 years of age or older has increased by 73,786,976,294,838,206,464,000 percent. The number of people 440 years of age or older has increased by 147,573,952,589,676,412,928,000 percent. The number of people 445 years of age or older has increased by 295,147,905,179,352,825,856,000 percent. The number of people 450 years of age or older has increased by 590,295,810,358,705,651,712,000 percent. The number of people 455 years of age or older has increased by 1,180,591,620,717,411,303,424,000 percent. The number of people 460 years of age or older has increased by 2,361,183,241,434,822,606,848,000 percent. The number of people 465 years of age or older has increased by 4,722,366,482,869,645,213,696,000 percent. The number of people 470 years of age or older has increased by 9,444,732,965,739,290,427,392,000 percent. The number of people 475 years of age or older has increased by 18,889,465,931,478,580,854,784,000 percent. The number of people 480 years of age or older has increased by 37,778,931,862,957,161,709,568,000 percent. The number of people 485 years of age or older has increased by 75,557,863,725,914,323,419,136,000 percent. The number of people 490 years of age or older has increased by 151,115,727,451,828,646,838,272,000 percent. The number of people 495 years of age or older has increased by 302,231,454,903,657,293,676,544,000 percent. The number of people 500 years of age or older has increased by 604,462,909,807,314,587,353,088,000 percent. The number of people 505 years of age or older has increased by 1,208,925,819,614,629,174,706,176,000 percent. The number of people 510 years of age or older has increased by 2,417,851,639,229,258,349,412,352,000 percent. The number of people 515 years of age or older has increased by 4,835,703,278,458,516,698,824,704,000 percent. The number of people 520 years of age or older has increased by 9,671,406,556,917,033,397,649,408,000 percent. The number of people 525 years of age or older has increased by 19,342,813,113,834,066,795,298,816,000 percent. The number of people 530 years of age or older has increased by 38,685,626,227,668,133,590,597,632,000 percent. The number of people 535 years of age or older has increased by 77,371,252,455,336,267,181,195,264,000 percent. The number of people 540 years of age or older has increased by 154,742,504,910,672,534,362,390,528,000 percent. The number of people 545 years of age or older has increased by 309,485,009,821,345,068,724,781,056,000 percent. The number of people 550 years of age or older has increased by 618,970,019,642,690,137,449,562,112,000 percent. The number of people 555 years of age or older has increased by 1,237,940,039,285,380,274,899,124,224,000 percent. The number of people 560 years of age or older has increased by 2,475,880,078,570,760,549,798,248,448,000 percent. The number of people 565 years of age or older has increased by 4,951,760,157,141,521,099,596,496,896,000 percent. The number of people 570 years of age or older has increased by 9,903,520,314,283,042,199,193,993,792,000 percent. The number of people 575 years of age or older has increased by 19,807,040,

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]


[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] image below. Each
of these pieces of information reflects user-identifying information.



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Abstract

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

© 2006 The Authors
Journal compilation © 2006 Blackwell Publishing Ltd

1. The first step in the process is to identify the problem. This involves gathering information about the situation and understanding the needs of the stakeholders involved.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible][illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

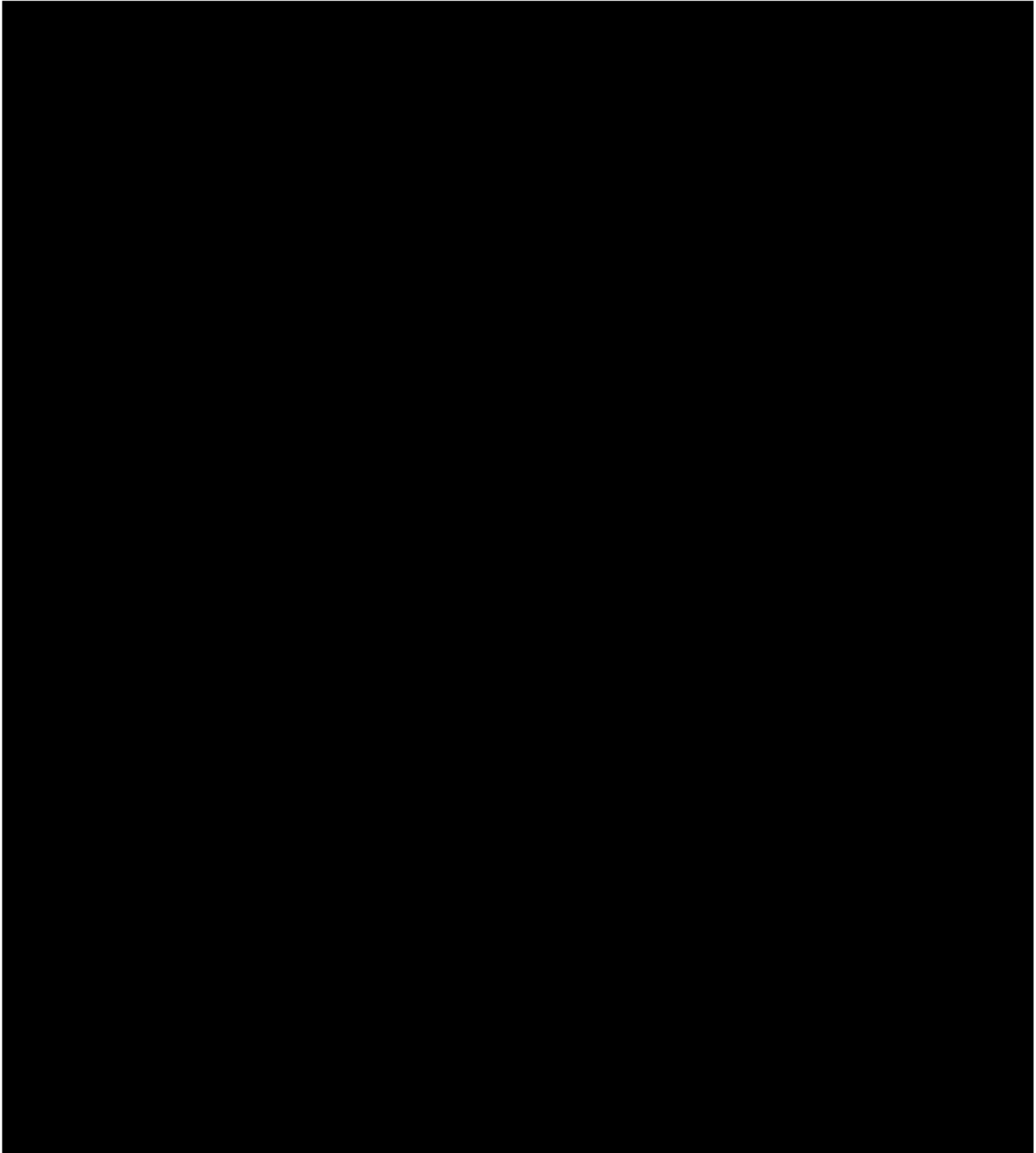
| [REDACTED]
| [REDACTED]
| [REDACTED]
[REDACTED]
| [REDACTED]
| [REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

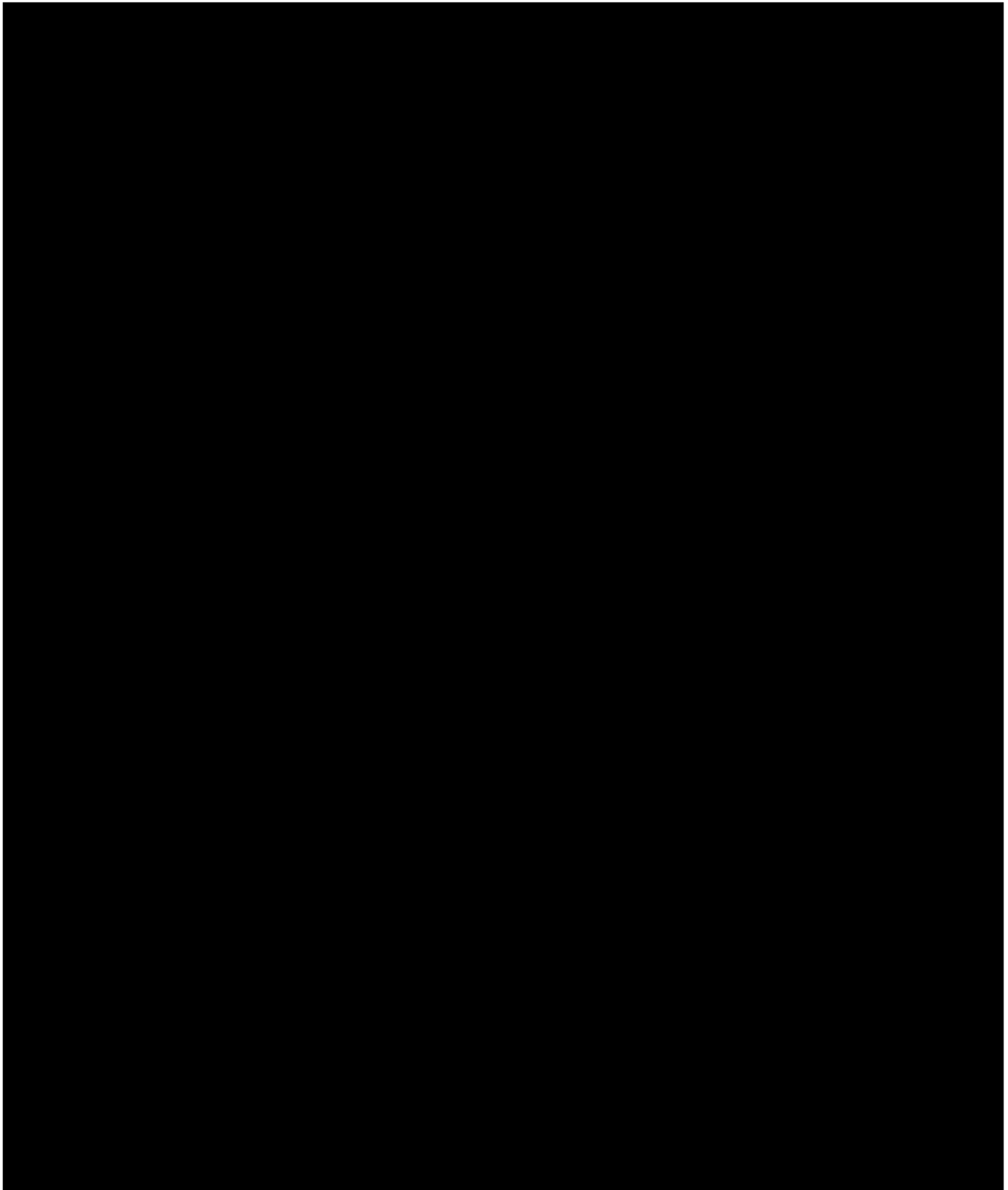
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

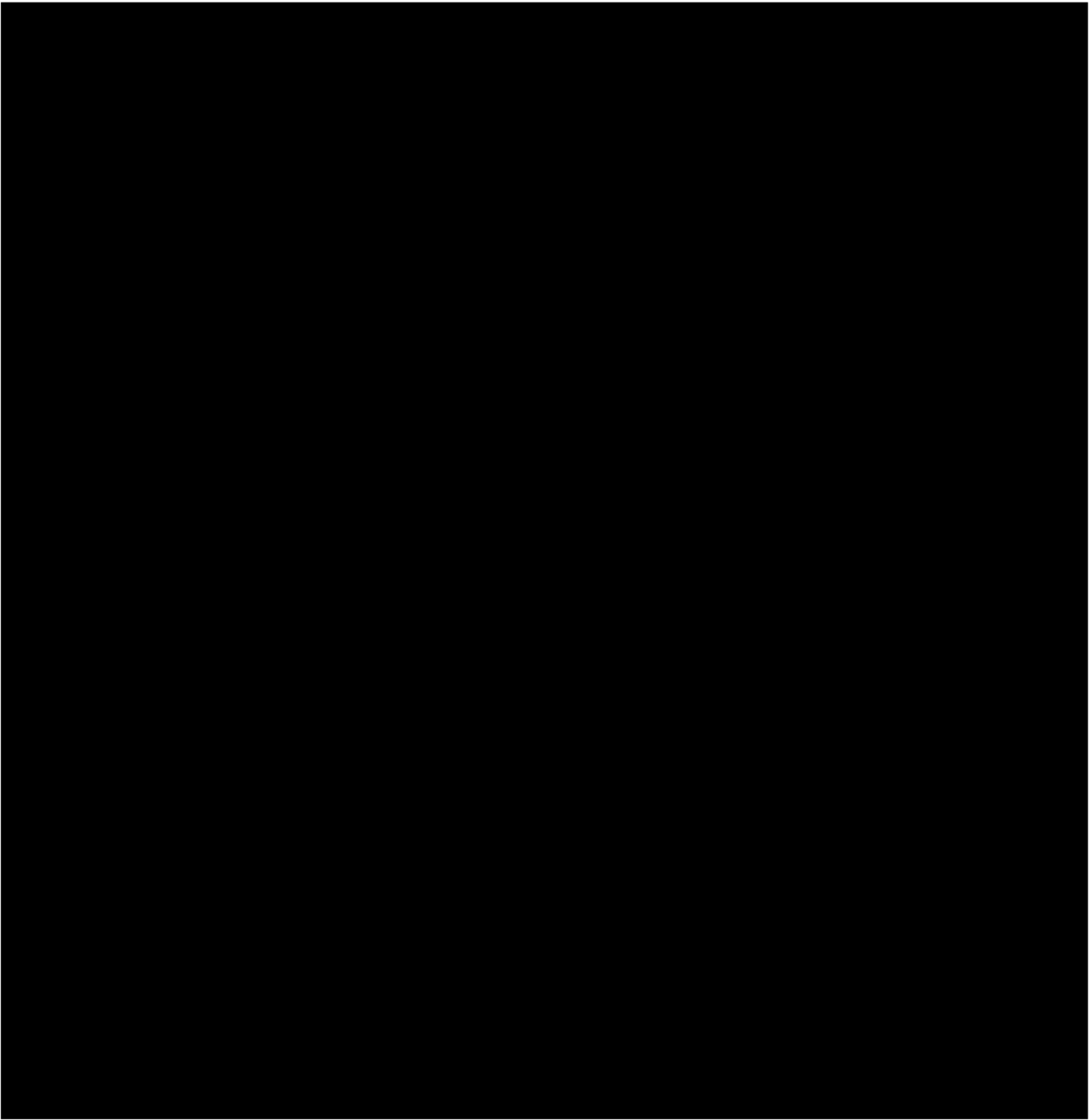
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

263 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

□

[REDACTED]

1. [REDACTED]
2. [REDACTED]
3. [REDACTED]
4. [REDACTED]
5. [REDACTED]
6. [REDACTED]
7. [REDACTED]
8. [REDACTED]
9. [REDACTED]
10. [REDACTED]
11. [REDACTED]
12. [REDACTED]
13. [REDACTED]
14. [REDACTED]
15. [REDACTED]
16. [REDACTED]
17. [REDACTED]
18. [REDACTED]
19. [REDACTED]
20. [REDACTED]
21. [REDACTED]
22. [REDACTED]
23. [REDACTED]
24. [REDACTED]
25. [REDACTED]
26. [REDACTED]
27. [REDACTED]
28. [REDACTED]
29. [REDACTED]
30. [REDACTED]
31. [REDACTED]
32. [REDACTED]
33. [REDACTED]
34. [REDACTED]
35. [REDACTED]
36. [REDACTED]
37. [REDACTED]
38. [REDACTED]
39. [REDACTED]
40. [REDACTED]
41. [REDACTED]
42. [REDACTED]
43. [REDACTED]
44. [REDACTED]
45. [REDACTED]
46. [REDACTED]
47. [REDACTED]
48. [REDACTED]
49. [REDACTED]
50. [REDACTED]
51. [REDACTED]
52. [REDACTED]
53. [REDACTED]
54. [REDACTED]
55. [REDACTED]
56. [REDACTED]
57. [REDACTED]
58. [REDACTED]
59. [REDACTED]
60. [REDACTED]
61. [REDACTED]
62. [REDACTED]
63. [REDACTED]
64. [REDACTED]
65. [REDACTED]
66. [REDACTED]
67. [REDACTED]
68. [REDACTED]
69. [REDACTED]
70. [REDACTED]
71. [REDACTED]
72. [REDACTED]
73. [REDACTED]
74. [REDACTED]
75. [REDACTED]
76. [REDACTED]
77. [REDACTED]
78. [REDACTED]
79. [REDACTED]
80. [REDACTED]
81. [REDACTED]
82. [REDACTED]
83. [REDACTED]
84. [REDACTED]
85. [REDACTED]
86. [REDACTED]
87. [REDACTED]
88. [REDACTED]
89. [REDACTED]
90. [REDACTED]
91. [REDACTED]
92. [REDACTED]
93. [REDACTED]
94. [REDACTED]
95. [REDACTED]
96. [REDACTED]
97. [REDACTED]
98. [REDACTED]
99. [REDACTED]
100. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

11/11/2016

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[illegible]

■ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

³⁰² As discussed in conjunction with the UpVoice app, UpVoice offers rewards for using the app.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

■ [REDACTED]
■ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

1	1	1	1	1
2	2	2	2	2
3	3	3	3	3
4	4	4	4	4
5	5	5	5	5
6	6	6	6	6
7	7	7	7	7
8	8	8	8	8
9	9	9	9	9
10	10	10	10	10
11	11	11	11	11
12	12	12	12	12
13	13	13	13	13
14	14	14	14	14
15	15	15	15	15
16	16	16	16	16
17	17	17	17	17
18	18	18	18	18
19	19	19	19	19
20	20	20	20	20
21	21	21	21	21
22	22	22	22	22
23	23	23	23	23
24	24	24	24	24
25	25	25	25	25
26	26	26	26	26
27	27	27	27	27
28	28	28	28	28
29	29	29	29	29
30	30	30	30	30
31	31	31	31	31
32	32	32	32	32
33	33	33	33	33
34	34	34	34	34
35	35	35	35	35
36	36	36	36	36
37	37	37	37	37
38	38	38	38	38
39	39	39	39	39
40	40	40	40	40
41	41	41	41	41
42	42	42	42	42
43	43	43	43	43
44	44	44	44	44
45	45	45	45	45
46	46	46	46	46
47	47	47	47	47
48	48	48	48	48
49	49	49	49	49
50	50	50	50	50
51	51	51	51	51
52	52	52	52	52
53	53	53	53	53
54	54	54	54	54
55	55	55	55	55
56	56	56	56	56
57	57	57	57	57
58	58	58	58	58
59	59	59	59	59
60	60	60	60	60
61	61	61	61	61
62	62	62	62	62
63	63	63	63	63
64	64	64	64	64
65	65	65	65	65
66	66	66	66	66
67	67	67	67	67
68	68	68	68	68
69	69	69	69	69
70	70	70	70	70
71	71	71	71	71
72	72	72	72	72
73	73	73	73	73
74	74	74	74	74
75	75	75	75	75
76	76	76	76	76
77	77	77	77	77
78	78	78	78	78
79	79	79	79	79
80	80	80	80	80
81	81	81	81	81
82	82	82	82	82
83	83	83	83	83
84	84	84	84	84
85	85	85	85	85
86	86	86	86	86
87	87	87	87	87
88	88	88	88	88

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

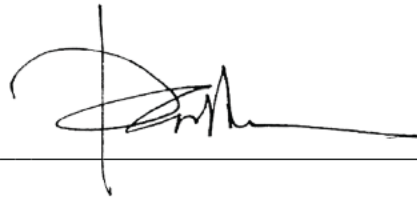
[REDACTED]

[REDACTED]

[REDACTED]

I declare, under penalty of perjury, that the foregoing is true and accurate.

DATED: January 12, 2022

A handwritten signature in black ink, appearing to read 'David Martens', is written over a horizontal line.

David Martens

Appendix A

David Martens

(415) 235-8886 – dave@intuityconsultants.com

Education

Stanford University, MS in Electrical Engineering (emphasis in comp. architecture, software, and circuits)
University of Wisconsin, Platteville, BS in Electrical Engineering
Santa Clara University, JD (emphasis in IP law)

Employment

Intuity Consultants, Inc. and Intuity, P.C. Software and Hardware Consultant and Attorney	11 Digital Drive, Suite B, Novato, CA July 2016 – present
Winston & Strawn LLP Attorney	San Francisco, CA 2013-2016
Finnegan, Henderson, Farabow, Garrett & Dunner LLP Attorney and Student Associate	Palo Alto, CA 2008 – 2013
Nixon & Peabody, LLP Summer Associate and Law Clerk	San Francisco, CA 2007-2008
Expressed Innovation, Inc. Software and Hardware Consultant	San Francisco Bay Area, CA 2005-2007
Sun Microsystems Engineering Manager, Technical Lead, and Design Engineer	Sunnyvale, CA 1998 – 2004
IBM Design Engineer	Austin, TX 1995 - 1998
Intel Design and Development Engineer	Sacramento, CA 1990 – 1995

Professional Society Memberships

IEEE (Solid State Circuits and Computer Societies); ACM

Litigations and Clients (last ten years)

Facebook v. BrandTotal, Ltd. and Unimania, Inc.; 3:20-cv-07182; Northern District of California; engaged by Wilmer Hale for Facebook; 2021-22

802 Systems v. Cisco Systems, Inc.; 2:20-cv-00315; Eastern District of Texas; engaged by Winston & Strawn LLP for Cisco; 2021

Streamscale, Inc. v. Intel Corp.; 6:21-cv-00198; Northern District of California; engaged by Wilmer Cutler Pickering Hale and Dorr for Intel; 2021

Zoho Corp. Pvt. Ltd. v. Freshworks, Inc.; Northern District of California; 3:20-cv-01869; engaged by Keker, Van Nest and Peters, LLP for Freshworks; 2021

Peters et al. v. Infor, Inc.; 3:19-cv-08102; Northern District of California; engaged by Keker, Van Nest and Peters for Infor; 2021

Stross, Ledergerber, Walmsley and Kuhmstetd v. Netease (four related cases); 2:20-cv-00861, 862, 863 and 2044; Central District of California; engaged by Doniger Burroughs; 2021

Teradata Corp. v. SAP et. al.; 3:18-cv-03670; Northern District of California; engaged by Morrison & Foerster for Teradata; 2021

Onstream Media Corp. v. Facebook; 6:19-cv-00708; Western District of Texas; engaged by Latham Watkins for Facebook; 2021

Via Vadis et al. v. Amazon (1:14-cv-810) and *Via Vadis et al. v. Blizzard Entertainment*; Western District of Texas; engaged by Perkins Coie for Amazon and Blizzard; 2021

DZ Reserve v. Facebook et al., 3:18-cv-04978; Northern District of California; engaged by Latham Watkins for Facebook; 2020

MasterObjects v. Facebook, 6:20-cv-00087; Western District of Texas; engaged by Latham & Watkins for Facebook; 2020-21

Exafer v. Microsoft, 6:19-cv-00687; Western District of Texas; engaged by Winston & Strawn for Microsoft; 2020-21

Voxer and Voxer IP, LLC v. Facebook and Instagram, 6:20-cv-00011; Western District of Texas; engaged by Kecker, Van Nest and Peters for Facebook; 2020-21

UMG v. Bright House Networks, 8:19-cv-710; Middle District of Florida; *Warner Records v. Charter Communications*, 19-cv-00874; District of Colorado; engaged by Winston & Strawn for Bright House Networks and Charter Communications; 2020-21

NexStep v. Comcast, 1:19-cv-01031; District of Delaware; engaged by Wilmer Hale for Comcast; 2020-21

XMTT, Inc. v. Intel Corporation, 1:18-cv-01810; District of Delaware; engaged by Desmarais IP for Intel; 2020

Pre-litigation assistance to AirBNB; engaged by Winston & Strawn; 2020

SpaceTime3D v. Samsung, 2:19-cv-00372; Eastern District of Texas; engaged by Susman Godfrey for SpaceTime3D; 2019-20

ARENDI S.A.R.L. v. Motorola Mobility, C.A. No. 12-1601; District of Delaware as well as *ARENDI S.A.R.L. v. LG Electronics et al.*, C.A. No. 12-1595, *ARENDI S.A.R.L. v. Apple, Inc.*, C.A. No. 12-1596, *ARENDI S.A.R.L. v. Blackberry*, C.A. No. 12-1597, *ARENDI S.A.R.L. v. Nokia et al.*, C.A. No. 12-1599, *ARENDI S.A.R.L. v. Sony et al.*, C.A. No. 12-1602, and *ARENDI S.A.R.L. v. Yahoo!/Verizon*, C.A. No. 13-0920; engaged by Susman Godfrey for ARENDI; 2019-20

Promptu Systems Corp. v. Comcast Corp., 2:16-cv-06516-LDD, Eastern District of Pennsylvania; engaged by Kecker, Van Nest & Peters for Comcast; 2019-21

Vir2us, Inc. v. Sophos, Inc., Sophos Ltd., Sophos Group PLC and Invincea, Inc., 2:19-cv-00018; Eastern District of Virginia; engaged by Bartko Zankel for Vir2us; 2019

Tabaian v. Intel, Inc., 3:18-cv-326; District of Oregon; engaged by Wilmer Hale for Intel; 2019

Resideo Techs. v. Ubiquitous Connectivity, IPR2019-01335 and -01336; engaged by Heninger, Garrison & Davis for Ubiquitous Connectivity; 2020

Askeladden v. Electronic Receipts Delivery Systems, IPR2020-01406 and -01407; engaged by Amster, Rothstein & Ebenstein; 2020

X-One, Inc. v. Uber Technologies, Inc., 1:16-cv-06050; Northern District of California; engaged by Finnegan Henderson for X-One; 2019

Rovi Guides, Inc. v. Comcast; 337-TA-1158 ITC investigation plus companion case in the Central District of California (2:19-CV-00275); engaged by Davis Polk for Comcast; 2019

LeadFactors v. Cisco, 1:13-CV-24792; Superior Court for the County of Santa Clara, California; engaged by Winston & Strawn for Cisco; 2019

Realtime Adaptive Streaming LLC v. Comcast, 1:18-CV-01446; District of Colorado; engaged by Farella Braun + Martell LLP for Comcast; 2019-21

Motorola Solutions v. Hytera Comm's Corp. Ltd. and Hytera Comm's (Australia) Pty Ltd., Federal Court of Australia Proceeding No. 1283/2017; engaged by Shelston IP for Hytera; 2019

Motorola Solutions v. Hytera Communications, 1:17-cv-01973; Northern District of Illinois; engaged by Steptoe and Johnson for Hytera; 2018-19

VLSI Technology v. Intel, 1:18-cv-00966; District of Delaware; engaged by Wilmer Hale for Intel; 2018

Rovi/TiVo/Veeco v. Comcast; 337-TA-1103 ITC investigation plus companion cases in the Central District of California (2:18-CV-00253) and District of Massachusetts (1:18-CV-10056); engaged by Davis Polk, Latham & Watkins, and Winston & Strawn for Comcast; 2018

Seven Networks v. Google; 2:17-CV-00442; ED of Texas; engaged by Quinn Emanuel for Google; 2018

Non-litigation legal analysis for Intel on microprocessor circuit technology; 2018

VLSI Technology v. Intel, 5:17-cv-05671; ND of California; engaged by Wilmer Hale for Intel; 2018

Arya Risk Management Systems v. Dufossat Capital Puerto Rico and Ashton Soniat; 4:16-CV-03595; Southern District of Texas; engaged by Heygood, Orr & Pearson for Arya Risk Management; 2018

Ubiquitous Connectivity v. City of San Antonio; 5:18-c-00718; Western District of Texas; engaged by Heninger Garrison Davis for Ubiquitous Connectivity; 2018

Non-litigation technical analysis of products for Salesforce; 2018

MacroPoint, LLC v. Ruiz Food Products, Inc.; 6:16-CV-01133; Eastern District of Texas; engaged by Thompson Hine, LLP for MacroPoint, 2018

OpenTV et al. v. Comcast Corp. et al., 337-TA-1041 ITC investigation plus companion cases in the Northern District of California (5:16-cv-06180-NC) and Eastern District of Texas (2:16-cv-01362); engaged by Kecker, Van Nest & Peters and WilmerHale for Comcast; 2017

Acceleration Bay v. Electronic Arts/TakeTwo/Activision; 1:16-cv-00454; District of Delaware; engaged by Winston & Strawn for EA/Activision/TakeTwo; 2017-18

Vir2us v. Cisco; 4:16-cv-06988; Northern District of California; engaged by Bunsow De Mory for Vir2us, 2017

Umbanet v. Epsilon Data Mgmt.; 2:16-cv-682; Eastern District of Texas; engaged by Spence PC for Umbanet; 2017

Rovi et al. v. Comcast, 337-TA-1001 ITC investigation plus companion case in Southern District of New York (1:16-cv-09278-JPO); engaged by Winston & Strawn for Comcast; 2016-18

Non-litigation legal analysis relating to USB technology for HP, Inc.; 2017-18

Ericsson v. Apple, 337-TA-952 ITC investigation; represented Ericsson while at Winston & Strawn; 2015

Non-litigation analysis relating to integrated circuit fabrication technology for TSMC while at Winston & Strawn; 2015

Macronix v. Spansion, 337-TA-909 ITC investigation; represented Macronix while at Winston & Strawn; 2013-14

Spansion v. Macronix, 337-TA-893 ITC investigation; represented Macronix while at Winston & Strawn; 2013-14

VIA Technologies v. Apple, 337-TA-812 ITC investigation; represented VIA Technologies while at Finnegan; 2011-12

Brocade Communications Systems, Inc. v. A10 Networks, Inc., 10-CV-03428, Northern District of California; represented A10 Networks while at Finnegan; 2011-12

EIDOS Display, LLC et al v. AU Optronics Corp. et al, 6:11-CV-00201, Eastern District of Texas; represented Hann-Star Display Corp. while at Finnegan, 2011-12

Keranos v. Analog Devices, Inc. et al, 2:10-cv-00207-TJW, Eastern District of Texas; represented Winbond while at Finnegan, 2011

PT Diagnostics, LLC v. Honeywell Int'l, Inc. et al, 2:10-cv-00493, Eastern District of Texas; represented QinetiQ North America while at Finnegan, 2010-2011

RAMBUS v. Freescale et al., 337-TA-753 ITC investigation; represented RAMBUS while at Finnegan; 2010-11

Appearances in Deposition or at Trial (Last 5 Years)

Peters et al. v. Infor, Inc.; 3:19-cv-08102; Northern District of California; engaged by Keker, Van Nest and Peters for Infor; 2021 (expert report; was deposed)

Stross, Ledergerber, Walmsley and Kuhmstedt v. Netease (four related cases); 2:20-cv-00861, 862, 863 and 2044; Central District of California; engaged by Doniger Burroughs; 2021 (expert report; was deposed)

Vir2us, Inc. v. Sophos, Inc., Sophos Ltd., Sophos Group PLC and Invincea, Inc., 2:19-cv-00018; Eastern District of Virginia; engaged by Bartko Zankel for Vir2us; 2019 (expert report and declaration; was deposed; went to trial but case resolved by summary judgment before my testimony at trial)

Engagements Involving an Expert Report or Declaration (Last 5 Years)

Facebook v. BrandTotal, Ltd. and Unimania, Inc.; 3:20-cv-07182; Northern District of California; engaged by Wilmer Hale for Facebook; 2021-22 (expert report)

Stross, Ledergerber, Walmsley and Kuhmstetd v. Netease (four related cases); 2:20-cv-00861, 862, 863 and 2044; Central District of California; engaged by Doniger Burroughs; 2021 (expert report; was deposed)

Vir2us, Inc. v. Sophos, Inc., Sophos Ltd., Sophos Group PLC and Invincea, Inc., 2:19-cv-00018; Eastern District of Virginia; engaged by Bartko Zankel for Vir2us; 2019 (expert report and declaration; was deposed; went to trial but case resolved by summary judgment before my testimony at trial)

Arya Risk Management Systems v. Dufossat Capital Puerto Rico and Ashton Soniat, 4:16-CV-03595; Southern District of Texas; engaged by Heygood, Orr & Pearson for Arya Risk Management; 2018 (expert report)

Patents (No Ownership Interest)

- 6,233,642 – Method for wiring a 64-bit rotator to maximize performance and minimize area
- 6,111,434 – Chargeshare protection for domino circuits
- 5,970,512 – Method for creating a faster lookup in microprocessor translation look-aside buffer
- 5,907,866 – Block Address Translation comparison circuit translator
- 5,864,571 – Error detection circuit with encoder
- 5,751,727 – Dynamic latch for use in dynamic memory arrays

Appendix B

[illegible]

Appendix C

[illegible]

[illegible]

Appendix D

Appendix D**A. Documents Produced by the Parties**

Documents Produced by BrandTotal	
BT0000114	BT0002878
BT0000132	BT0002879
BT0000159	BT0002880
BT0000378	BT0002881
BT0000524	BT0002882
BT0000806	BT0002883
BT0000807	BT0002884
BT0000808	BT0002946
BT0000809	BT0002947
BT0001432	BT0002948
BT0001485	BT0002949
BT0001492	BT0002954
BT0001493	BT0002959
BT0001498	BT0002988
BT0001552	BT0002989
BT0001554	BT0005330
BT0001555	BT0005331
BT0001560	BT0005332
BT0001889	BT0005333
BT0001890	BT0005334
BT0001891	BT0005409
BT0001892	BT0005410
BT0001893	BT0005476
BT0001894	BT0005479
BT0001895	BT0005482
BT0001896	BT0005484
BT0001897	BT0005485
BT0001898	BT0005486
BT0001899	BT0005490
BT0001900	BT0005496
BT0001901	BT0005514
BT0001902	BT0005516
BT0001903	BT0005524
BT0001904	BT0005541
BT0001905	BT0005542
BT0001906	BT0005543
BT0001907	BT0005546
BT0001908	BT0005550
BT0001909	BT0005552
BT0002871	BT0005553
BT0002872	BT0005556
BT0002873	BT0005557
BT0002874	BT0005558
BT0002875	BT0005560
BT0002876	BT0005562
BT0002877	BT0005565
Documents Produced by Meta	
FB BRTL 00001166	

B. Pleadings and DiscoveryPleadings

- 2020-12-23 Defendants/Counterclaim Plaintiffs Objections and Responses to Plaintiff/Counterclaim Defendant Request for Interrogatories to BrandTotal Ltd. and Unimania
- 2021-02-23 Plaintiff/Counterclaim Defendant Request for Interrogatories to BrandTotal Ltd. and Unimania
- 2021-04-26 Defendants/Counterclaim Plaintiffs Objections and Responses to Plaintiff/Counterclaim Defendant's Request for Interrogatories to BrandTotal Ltd. and Unimania
- 2021-05-18 Defendants/Counterclaim Plaintiffs Objections and Responses to Plaintiff/Counterclaim Defendant's Request for Interrogatories to BrandTotal Ltd. and Unimania
- 2021-05-24 First Amended Complaint; Demand for Jury Trial
- 2021-11-05 Plaintiff/Counterclaim Defendant Objections and Responses to Defendants/Coutnerclaim Plaintiffs' Request for Interrogatories to BrandTotal Ltd. and Unimania

Depositions

- 2021-01-13 Deposition of Oren Dor, Former Vice President of R&D at BrandTotal, and Exhibits
- 2021-01-13 Deposition of Sanchit Karve, Malware Researcher at Meta
- 2021-03-10 Deposition of Oren Dor, Former Vice President of R&D at BrandTotal, and Exhibits
- 2021-11-18 Deposition of Yair Regev, Vice President of R&D at BrandTotal

Declarations

- 2021-03-12 Decl. of Robert Sherwood ISO Defendant's Renewed Mot. For Preliminary Injunction
- 2021-03-12 Decl. of Professor Woodrow Hartzog ISO Defendant's Renewed Mot. For Preliminary Injunction

C. BrandTotal Database Queries

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

D. Rapid7 Logs

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

E. BrandTotal Source Code

BT-CODE-0000011	BT-CODE-0000549
BT-CODE-0000024	BT-CODE-0000556
BT-CODE-0000123	BT-CODE-0000561
BT-CODE-0000170	BT-CODE-0000562
BT-CODE-0000193	BT-CODE-0000572
BT-CODE-0000204	BT-CODE-0000639
BT-CODE-0000206	BT-CODE-0000659
BT-CODE-0000233	BT-CODE-0000795
BT-CODE-0000340	BT-CODE-0000812
BT-CODE-0000345	BT-CODE-0000819
BT-CODE-0000452	BT-CODE-0000856
BT-CODE-0000452	BT-CODE-0000894
BT-CODE-0000519	BT-CODE-0000948
BT-CODE-0000548	BT-CODE-0000967

F. Additional Productions

[illegible]

G. Information from Public Sources

Graph Theory Article on Science Direct (https://www.sciencedirect.com/topics/earth-and-planetary-sciences/graph-theory)	Facebook's Access Token Debugger (https://developers.facebook.com/tools/debug/accesstoken/)
Nielsen's Definition for DMA (https://www.nielsen.com/us/en/contact-us/intl-campaigns/dma-maps)	Article titled Android users now face forced app updates, thank sot Google's new dev tools on ZD Net (https://www.zdnet.com/article/android-users-now-face-forced-app-updates-thanks-to-googles-new-dev-tools/)
Rapid7 Website (www.rapid7.com)	Fiddler's Website (https://www.telerik.com/fiddler)
Amazon AWS Information Page (https://aws.amazon.com/what-is-aws/)	Google Chrome Store (https://chrome.google.com/webstore/category/extensions)
Amazon AWS Server (https://aws.amazon.com/serverless/)	How to Install Chrome Extensions Manually (https://www.cnet.com/tech/services-and-software/how-to-install-chrome-extensions-manually/)
Amazon AWS SQS (https://aws.amazon.com/sqs/)	LinkedIn of Liram Vardi
Amazon AWS RDS (https://aws.amazon.com/rds/)	Rate Limits for Meta Developers (https://developers.facebook.com/docs/graph-api/overview/rate-limiting/)
Restricted Content Within Facebook (https://www.facebook.com/policies/ads/restricted_content)	In-app Updates on Android Developer (https://developer.android.com/guide/playcore/in-app-updates)
Restricted Content Within Instagram (https://help.instagram.com/801322493288277)	IP 2 Location Demo (https://www.ip2location.com/demo/18.205.36.100)
Hamms the Beer Post (https://www.facebook.com/HammsTheBeer/photos/a.335653770261098/1233626893797110/)	Android Developer Documentation for Cookie Manager (https://developer.android.com/reference/android/webkit/CookieManager)
Heineken Mexico Page (https://www.facebook.com/HEINEKENMexico)	Introduction to Code Obfuscation on Better Programming (https://betterprogramming.pub/code-obfuscation-introduction-to-code-obfuscation-part-1-93a6797349b0)

EXHIBIT 19

REDACTED VERSION OF
EXHIBIT FILED UNDER
SEAL

HIGHLY CONFIDENTIAL - ATTORNEYS' EYES ONLY

Page 1

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

META PLATFORMS, INC., a : Case No.
Delaware corporation : 3:20-CV-07182-JCS
:
Plaintiff/Counterclaim :
Defendant :
:
vs. :
:
BRANDTOTAL, LTD., an :
Israel corporation, and :
UNIMANIA, INC., a Delaware :
corporation :
:
Defendants/Counterclaim :
Plaintiffs :

SUNDAY, FEBRUARY 20, 2022
HIGHLY CONFIDENTIAL
ATTORNEYS' EYES ONLY
CONTAINS SOURCE CODE

Remote Videotape Zoom Deposition of LIRAM
VARDI, taken pursuant to Notice, in Shorashim,
Israel, commencing at approximately 3:04 p.m.,
Israel time, on the above date, before Rose A.
Tamburri, RPR, CM, CCR, CRR, USCRA Speed and
Accuracy Champion and Notary Public.

VERITEXT LEGAL SOLUTIONS
Mid-Atlantic Region
1801 Market Street - Suite 1800
Philadelphia, Pennsylvania 19103

1

13 (Pages 46 - 49)

Page 52

[illegible]

Page 53

[illegible]

Page 100

[illegible][illegible]

Page 101

[illegible][illegible]

HIGHLY CONFIDENTIAL - ATTORNEYS' EYES ONLY

<div>1 [REDACTED]</div> <div>Page 102</div>	<div>Page 104</div> <div>[REDACTED]</div>
<div>1 [REDACTED]</div> <div>Page 103</div>	<div>Page 105</div> <div>[REDACTED]</div>

HIGHLY CONFIDENTIAL - ATTORNEYS' EYES ONLY

<div>Page 142</div> <div>1 [REDACTED]</div>	<div>[REDACTED]</div> <div>1 [REDACTED]</div>
<div>Page 143</div> <div>1 [REDACTED]</div>	<div>[REDACTED]</div> <div>[REDACTED]</div>

[illegible]

HIGHLY CONFIDENTIAL - ATTORNEYS' EYES ONLY

<div>1</div> <div>Page 150</div> <div>[REDACTED]</div>	<div>[REDACTED]</div>
<div>[REDACTED]</div>	<div>[REDACTED]</div>

1 Q. Does BrandTotal use residential

[illegible][illegible][illegible][illegible]

[illegible]

1

46 (Pages 178 - 181)

HIGHLY CONFIDENTIAL - ATTORNEYS' EYES ONLY

Page 182

1 email, some point after this email.
2 Q. At some point after this email in
3 June of 2021, you started using the restricted
4 panel extension?
5 A. Yes, because this is like part of the
6 development process, I think.
7 Q. Okay.
8 Was it after October 1st of 2021
9 that you started using the restricted panel
10 extension?
11 A. What is the date of this email?
12 Q. June of 2021.
13 A. June -- I think not too much after
14 this one.
15 Q. Just so I --
16 A. Again, I don't remember exactly, but
17 I think not too much after this. This is --
18 was part of the development process event.
19 Q. Did you collect any information from
20 restricted pages during the first six months
21 of 2021?
22 A. It's possible, yes.
23

[REDACTED]

Page 183

[illegible]

Page 184

[REDACTED]

Q. The restricted panel extension -- strike that.

A. The workers who were using the restricted panel extension to collect information from restricted pages, do they use a VPN?

A. I think that, yes, sometimes.

Q. Why -- why do they sometimes use a VPN?

A. Again, did you ask about the restricted panel extension?

Q. Yes.

A. Yes, because our worker is -- is --

Page 185

1 is in India and sometimes in order to see
2 posts from UK, you need to be in UK or using a
3 UK IP or in Mexico, for instance.
4 Q. So BrandTotal has hired a worker to
5 install the restricted panel extension on
6 their computer in India; correct?
7 A. Correct.
8 Q. And they have installed the
9 restricted panel extension and they log into
10 Facebook with their Facebook account; correct?
11 A. Correct.
12 Q. And then they use a VPN so it appears
13 that the request is coming from Mexico, for
14 example?
15 A. Correct.
16 Q. Or they use a VPN so it appears that
17 the request is coming from the UK, for
18 example?
19 A. I'm not sure about -- I'm not in the
20 product side, so I don't know -- sorry, in the
21 customer success, but it's possible.
22 Q. And if they didn't use a VPN, then
23 Facebook would not allow them to see the
24 restricted pages that they are trying to see?
25 MR. TAYLOR: Object to form.

HIGHLY CONFIDENTIAL - ATTORNEYS' EYES ONLY

Page 186

1 THE WITNESS: It depends. It
2 depends the page because I think it's not
3 related to Facebook. I think it's more
4 related to restriction in country or something
5 like this.

6 BY MR. HOLTZBLATT:

7 Q. The -- the VPN is necessary because
8 without the VPN, they wouldn't be able to see
9 the pages that they're -- you're trying to
10 collect information from?

11 A. No, it's more that we need to make
12 sure this is the posts that Mexican users see,
13 okay? So -- so the data would be more
14 reliable. Also, sometimes Facebook redirect
15 you to a page which is routed to your country,
16 for instance, India. So if you want to see,
17 for instance, some advertiser in Mexico and
18 you're from India, then Facebook doing a
19 redirect for you for India.

20 So this is -- now that I am
21 talking about it, I remember. This is the
22 main reason, okay? This is now I'm sure that
23 this is like the -- the answer for that.

24 Q. Please take a look at what I've
25 marked as Exhibit 12.

Page 188

[illegible]

Page 187

[illegible]

Page 189

1

49 (Pages 190 - 193)

1

50 (Pages 194 - 197)

HIGHLY CONFIDENTIAL - ATTORNEYS' EYES ONLY


<p style="text-align: right;">Page 202</p> <p>1 hit the four-hour point that the parties 2 agreed to in ECF No. 216 and it is our 3 position that this concludes the deposition 4 for today. 5 MR. HOLTZBLATT: And I will 6 register my objection that I believe that it 7 would be in the interest of the parties and 8 the efficient administration of this case to 9 agree to a short extension of the time of the 10 deposition. For that reason, I am leaving the 11 deposition open and I'm sorry, Mr. Vardi, that 12 may mean that we'll have to bring you back for 13 a short extension of the deposition, but that 14 was the choice of your counsel, not myself. 15 THE VIDEOGRAPHER: Okay. Shall I 16 take us off the record? 17 MR. TAYLOR: Yes. 18 MR. HOLTZBLATT: Yes. 19 THE VIDEOGRAPHER: Thank you. We 20 will be off the record at 8:16 p m. and this 21 will conclude today's testimony given by Liram 22 Vardi. Thank you. 23 (Whereupon, the deposition 24 adjourned at the above time.) 25</p>	
<p style="text-align: right;">Page 203</p> <p>1 CERTIFICATE 2 3 I do hereby certify that I am a 4 Notary Public in good standing, that the 5 aforesaid testimony was taken before me, 6 pursuant to notice, at the time and place 7 indicated; that said deponent was by me duly 8 sworn to tell the truth, the whole truth, and 9 nothing but the truth; that the testimony of 10 said deponent was correctly recorded in 11 machine shorthand by me and thereafter 12 transcribed under my supervision with 13 computer-aided transcription; that the 14 deposition is a true and correct record of the 15 testimony given by the witness; and that I am 16 neither of counsel nor kin to any party in 17 said action, nor interested in the outcome 18 thereof 19 20 WITNESS by hand and official seal 21 this 20th day of February, 2022 22 23 24 25</p> <div style="text-align: center;">  Rose Tamburri Notary Public </div>	

EXHIBIT 20

EXHIBIT FILED UNDER
SEAL